U.S.-Canada Power System Outage Task Force

Interim Report:

Causes of the August 14th Blackout in the United States and Canada

Canada

November 2003

U.S.-Canada Power System Outage Task Force

Interim Report:

Causes of the August 14th Blackout in the United States and Canada

November 2003

Acknowledgments

The U.S.-Canada Power System Outage Task Force would like to acknowledge all the researchers, analysts, modelers, investigators, planners, designers, and others for their time and effort spent on completing this Interim Report. The result is an international coordinated report providing factual reasons as to why the power outage occurred. This Interim Report was prepared for the U.S. Secretary of Energy and the Minister of Natural Resources Canada (NRCAN) under the direction of Jimmy Glotfelty (USDOE) and Dr. Nawal Kamel and the three working groups: electric system, nuclear, and security.

Members of the three working groups and investigative teams spent an incalculable number of hours researching in various locations to better understand the intricacies of the August 14, 2003, power outage. It was a huge endeavor to achieve, and they did an excellent job providing the facts though a variety of data requests; analysis of operations, generator and transmission modeling; sequence of events, and root cause analysis. Along with countless interviews and a variety of side investigations, the planning and preparation, coordinated internationally, all proved to be a confidently coordinated effort.

Thank you for spending countless hours on in-depth research and participating in a report that will help the North American public and the world better understand why and what caused the August 14, 2003, blackout. Your efforts are greatly appreciated! Thank you.

Contents

Appendixes

Page

Tables

Figures

Figures (Continued) **Page**

1. Introduction

On August 14, 2003, large portions of the Midwest and Northeast United States and Ontario, Canada, experienced an electric power blackout. The outage affected an area with an estimated 50 million people and 61,800 megawatts (MW) of electric load in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, and New Jersey and the Canadian province of Ontario. The blackout began a few minutes after 4:00 pm Eastern Daylight Time (16:00 EDT), and power was not restored for 2 days in some parts of the United States. Parts of Ontario suffered rolling blackouts for more than a week before full power was restored.

On August 15, President George W. Bush and Prime Minister Jean Chrétien directed that a joint U.S.-Canada Power System Outage Task Force be established to investigate the causes of the blackout and how to reduce the possibility of future outages. They named U.S. Secretary of Energy Spencer Abraham and Herb Dhaliwal, Minister of Natural Resources, Canada, to chair the joint Task Force. Three other U.S. representatives and three other Canadian representatives were named to the Task Force. The U.S. members are Tom Ridge, Secretary of Homeland Security; Pat Wood, Chairman of the Federal Energy Regulatory Commission; and Nils Diaz, Chairman of the Nuclear Regulatory Commission. The Canadian members are Deputy Prime Minister John Manley, Deputy Prime Minister; Kenneth Vollman, Chairman of the National Energy Board; and Linda J. Keen, President and CEO of the Canadian Nuclear Safety Commission.

The Task Force divided its work into two phases:

- Phase I: Investigate the outage to determine its causes and why it was not contained.
- Phase II: Develop recommendations to reduce the possibility of future outages and minimize the scope of any that occur.

The Task Force created three Working Groups to assist in the Phase I investigation of the blackout—an Electric System Working Group (ESWG), a Nuclear Working Group (NWG), and a Security Working Group (SWG). They were tasked with overseeing and reviewing investigations of the conditions and events in their respective areas and determining whether they may have caused or affected the blackout. The Working Groups are made up of State and provincial representatives, Federal employees, and contractors working for the U.S. and Canadian government agencies represented on the Task Force.

This document provides an Interim Report, forwarded by the Working Groups, on the findings of the Phase I investigation. It presents the facts that the bi-national investigation has found regarding the causes of the blackout on August 14, 2003. The Working Groups and their analytic teams are confident of the accuracy of these facts and the analysis built upon them. This report does not offer speculations or assumptions not supported by evidence and analysis. Further, it does not attempt to draw broad conclusions or suggest policy recommendations; that task is to be undertaken in Phase II and is beyond the scope of the Phase I investigation.

This report will now be subject to public review and comment. The Working Groups will consider public commentary on the Interim Report and will oversee and review any additional analyses and investigation that may be required. This report will be finalized and made a part of the Task Force Final Report, which will also contain recommendations on how to minimize the likelihood and scope of future blackouts.

The Task Force will hold three public forums, or consultations, in which the public will have the opportunity to comment on this Interim Report and to present recommendations for consideration by the Working Groups and the Task Force.

The public may also submit comments and recommendations to the Task Force electronically or by mail. Electronic submissions may be sent to:

poweroutage@nrcan.gc.ca
and
blackout.report@hq.doe.gov.

Paper submissions may be sent by mail to:

Dr. Nawal Kamel
Special Adviser to the Deputy Minister
Natural Resources Canada
21st Floor
580 Booth Street
Ottawa, ON K1A 0E4
and
Mr. James W. Glotfelty
Director, Office of Electric Transmission and Distribution
U.S. Department of Energy
1000 Independence Avenue, S.W.
Washington, DC 20585

This Interim Report is divided into eight chapters, including this introductory chapter:

- Chapter 2 provides an overview of the institutional framework for maintaining and ensuring the reliability of the bulk power system in North America, with particular attention to the roles and responsibilities of several types of reliability-related organizations.
- Chapter 3 discusses conditions on the regional power system before August 14 and on August 14 before the events directly related to the blackout began.
- Chapter 4 addresses the causes of the blackout, with particular attention to the evolution of conditions on the afternoon of August 14, starting from normal operating conditions, then going into a period of abnormal but still potentially manageable conditions, and finally into an uncontrollable cascading blackout.
- Chapter 5 provides details on the cascade phase of the blackout.
- Chapter 6 compares the August 14, 2003, blackout with previous major North American power outages.
- Chapter 7 examines the performance of the nuclear power plants affected by the August 14 outage.
- Chapter 8 addresses issues related to physical and cyber security associated with the outage.

This report also includes four appendixes: a description of the investigative process that provided the basis for this report, a list of electricity acronyms, a glossary of electricity terms, and three transmittal letters pertinent to this report from the three Working Groups.

2. Overview of the North American Electric Power System and Its Reliability Organizations

The North American Power Grid Is One Large, Interconnected Machine

The North American electricity system is one of the great engineering achievements of the past 100 years. This electricity infrastructure represents more than $1 trillion in asset value, more than 200,000 miles (320,000 kilometers) of transmission lines operating at 230,000 volts and greater, 950,000 megawatts of generating capability, and nearly 3,500 utility organizations serving well over 100 million customers and 283 million people.

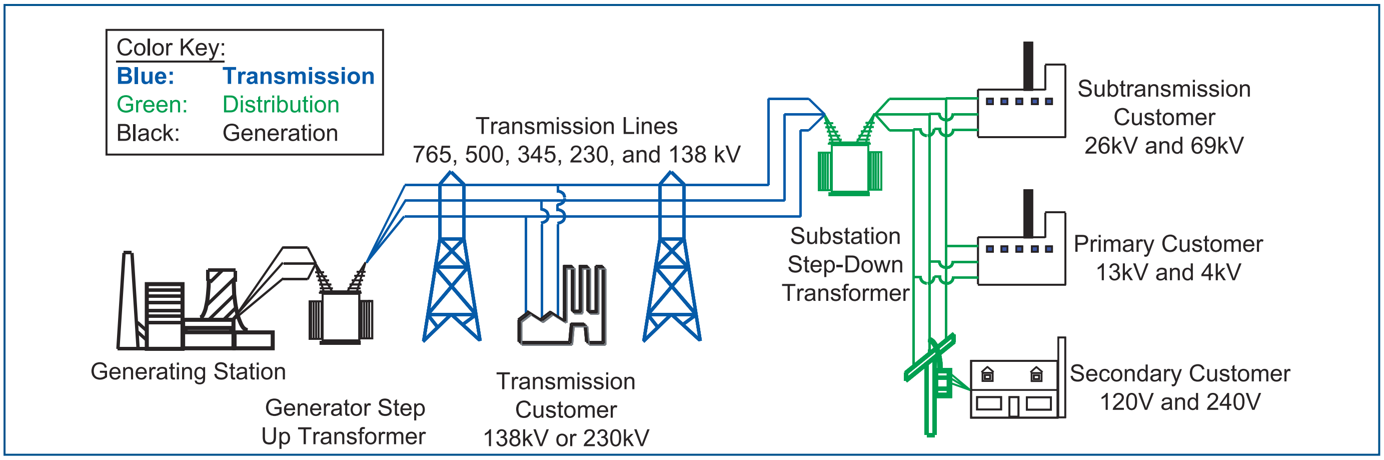
Modern society has come to depend on reliable electricity as an essential resource for national security; health and welfare; communications; finance; transportation; food and water supply; heating, cooling, and lighting; computers and electronics; commercial enterprise; and even entertainment and leisure—in short, nearly all aspects of modern life. Customers have grown to expect that electricity will almost always be available when needed at the flick of a switch. Most customers have also experienced local outages caused by a car hitting a power pole, a construction crew accidentally damaging a cable, or a lightning storm. What is not expected is the occurrence of a massive outage on a calm, warm day. Widespread electrical outages, such as the one that occurred on August 14, 2003, are rare, but they can happen if multiple reliability safeguards break down.

Providing reliable electricity is an enormously complex technical challenge, even on the most routine of days. It involves real-time assessment, control and coordination of electricity production at thousands of generators, moving electricity across an interconnected network of transmission lines, and ultimately delivering the electricity to millions of customers by means of a distribution network.

As shown in Figure 2.1, electricity is produced at lower voltages (10,000 to 25,000 volts) at generators from various fuel sources, such as nuclear, coal, oil, natural gas, hydro power, geothermal, photovoltaic, etc. Some generators are owned by the same electric utilities that serve the end-use customer; some are owned by independent power producers (IPPs); and others are owned by customers themselves—particularly large industrial customers.

Electricity from generators is “stepped up” to higher voltages for transportation in bulk over

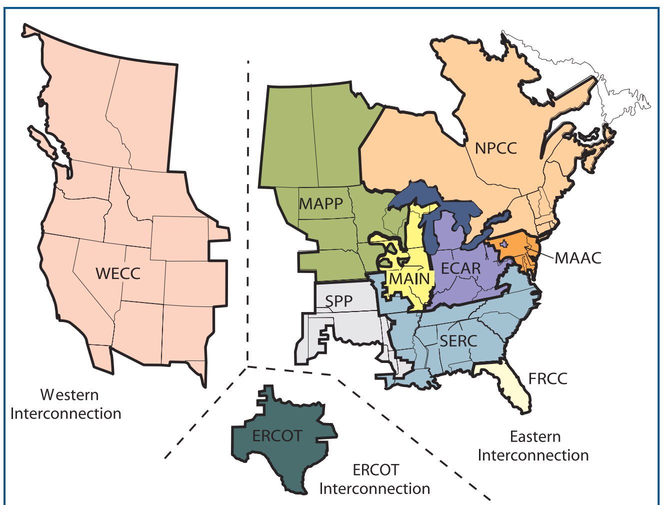
Figure 2.1. Basic Structure of the Electric System



transmission lines. Operating the transmission lines at high voltage (i.e., 230,000 to 765,000 volts) reduces the losses of electricity from conductor heating and allows power to be shipped economically over long distances. Transmission lines are interconnected at switching stations and substations to form a network of lines and stations called the power "grid." Electricity flows through the interconnected network of transmission lines from the generators to the loads in accordance with the laws of physics—along "paths of least resistance," in much the same way that water flows through a network of canals. When the power arrives near a load center, it is "stepped down" to lower voltages for distribution to customers. The bulk power system is predominantly an alternating current (AC) system, as opposed to a direct current (DC) system, because of the ease and low cost with which voltages in AC systems can be converted from one level to another. Some larger industrial and commercial customers take service at intermediate voltage levels (12,000 to 115,000 volts), but most residential customers take their electrical service at 120 and 240 volts.

While the power system in North America is commonly referred to as "the grid," there are actually three distinct power grids or "interconnections" (Figure 2.2). The Eastern Interconnection includes the eastern two-thirds of the continental United States and Canada from Saskatchewan east to the Maritime Provinces. The Western Interconnection includes the western third of the continental United States (excluding Alaska), the Canadian Provinces of Alberta and British Columbia, and a portion of Baja California Norte, Mexico. The third interconnection comprises most of the state of

Figure 2.2. NERC Interconnections



Texas. The three interconnections are electrically independent from each other except for a few small direct current (DC) ties that link them. Within each interconnection, electricity is produced the instant it is used, and flows over virtually all transmission lines from generators to loads.

The northeastern portion of the Eastern Interconnection (about 10 percent of the interconnection's total load) was affected by the August 14 blackout. The other two interconnections were not affected.[1]

Planning and Reliable Operation of the Power Grid Are Technically Demanding

Reliable operation of the power grid is complex and demanding for two fundamental reasons:

- First, electricity flows at the speed of light (186,000 miles per second or 297,600 kilometers per second) and is not economically storable in large quantities. Therefore electricity must be produced the instant it is used.
- Second, the flow of alternating current (AC) electricity cannot be controlled like a liquid or gas by opening or closing a valve in a pipe, or switched like calls over a long-distance telephone network. Electricity flows freely along all available paths from the generators to the loads in accordance with the laws of physics—dividing among all connected flow paths in the network, in inverse proportion to the impedance (resistance plus reactance) on each path.

Maintaining reliability is a complex enterprise that requires trained and skilled operators, sophisticated computers and communications, and careful planning and design. The North American Electric Reliability Council (NERC) and its ten Regional Reliability Councils have developed system operating and planning standards for ensuring the reliability of a transmission grid that are based on seven key concepts:

- Balance power generation and demand continuously.
- Balance reactive power supply and demand to maintain scheduled voltages.
- Monitor flows over transmission lines and other facilities to ensure that thermal (heating) limits are not exceeded.

- Keep the system in a stable condition.
- Operate the system so that it remains in a reliable condition even if a contingency occurs, such as the loss of a key generator or transmission facility (the "N-1 criterion").
- Plan, design, and maintain the system to operate reliably.
- Prepare for emergencies.

These seven concepts are explained in more detail below.

1. **Balance power generation and demand continuously.** To enable customers to use as much electricity as they wish at any moment, production by the generators must be scheduled or "dispatched" to meet constantly changing demands, typically on an hourly basis, and then fine-tuned throughout the hour, sometimes through the use of automatic generation controls to continuously match generation to actual demand. Demand is somewhat predictable, appearing as a daily demand curve—in the summer, highest during the afternoon and evening and lowest in the middle of the night, and higher on weekdays when most businesses are open (Figure 2.3).

   Failure to match generation to demand causes the frequency of an AC power system (nominally 60 cycles per second or 60 Hertz) to increase (when generation exceeds demand) or decrease (when generation is less than demand) (Figure 2.4). Random, small variations in frequency are normal, as loads come on and off and generators modify their output to follow the demand changes. However, large deviations in frequency can cause the rotational speed of generators to fluctuate, leading to vibrations that can damage generator turbine blades and other equipment. Extreme low frequencies can trigger automatic under-frequency "load shedding," which takes blocks of customers off-line in order to prevent a total collapse of the electric system. As will be seen later in this report, such an imbalance of generation and demand can also occur when the system responds to major disturbances by breaking into separate "islands"; any such island may have an excess or a shortage of generation, compared to demand within the island.

2. **Balance reactive power supply and demand to maintain scheduled voltages.** Reactive power sources, such as capacitor banks and generators, must be adjusted during the day to maintain voltages within a secure range pertaining to all system electrical equipment (stations, transmission lines, and customer equipment). Most generators have automatic voltage regulators that cause the reactive power output of generators to increase or decrease to control voltages to scheduled levels. Low voltage can cause electric system instability or collapse and, at distribution voltages, can cause damage to motors and the failure of electronic equipment. High voltages can exceed the insulation capabilities of equipment and cause dangerous electric arcs ("flashovers").

3. **Monitor flows over transmission lines and other facilities to ensure that thermal (heating) limits are not exceeded.** The dynamic interactions between generators and loads, combined with the fact that electricity flows freely across all interconnected circuits, mean that power flow is ever-changing on transmission and distribution lines. All lines, transformers, and other equipment carrying electricity are heated by the flow of electricity through them. The

Figure 2.3. PJM Load Curve, August 18-24, 2003

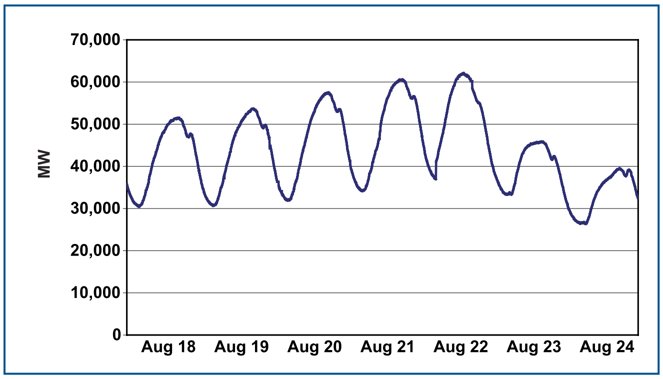
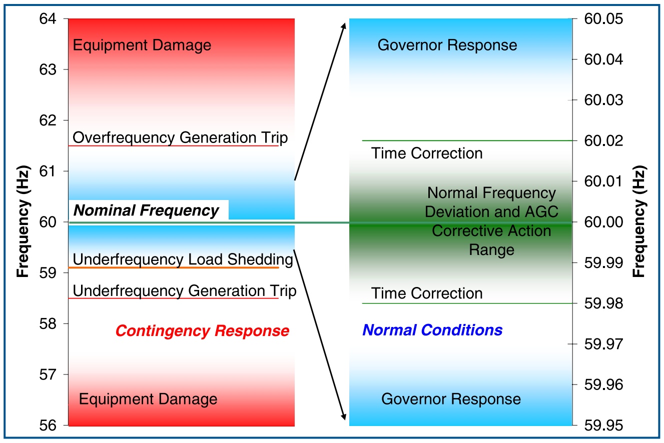


Figure 2.4. Normal and Abnormal Frequency Ranges



Local Supplies of Reactive Power Are Essential to Maintaining Voltage Stability

A generator typically produces some mixture of "active" and "reactive" power, and the balance between them can be adjusted at short notice to meet changing conditions. Active power, measured in watts, is the form of electricity that powers equipment. Reactive power, a characteristic of AC systems, is measured in volt-amperes reactive (VAr), and is the energy supplied to create or be stored in electric or magnetic fields in and around electrical equipment. Reactive power is particularly important for equipment that relies on magnetic fields for the production of induced electric currents (e.g., motors, transformers, pumps, and air conditioning.) Transmission lines both consume and produce reactive power. At light loads they are net producers, and at heavy loads, they are heavy consumers. Reactive power consumption by these facilities or devices tends to depress transmission voltage, while its production (by generators) or injection (from storage devices such as capacitors) tends to support voltage. Reactive power can be transmitted only over relatively short distances, and thus must be supplied as needed from nearby generators or capacitor banks. If reactive power cannot be supplied promptly and in sufficient quantity, voltages decay, and in extreme cases a "voltage collapse" may result.

flow must be limited to avoid overheating and damaging the equipment. In the case of overhead power lines, heating also causes the metal conductor to stretch or expand and sag closer to ground level. Conductor heating is also affected by ambient temperature, wind, and other factors. Flow on overhead lines must be limited to ensure that the line does not sag into obstructions below such as trees or telephone lines, or violate the minimum safety clearances between the energized lines and other objects. (A short circuit or "flashover"—which can start fires or damage equipment—can occur if an energized line gets too close to another object). All electric lines, transformers and other current-carrying devices are monitored continuously to ensure that they do not become overloaded or violate other operating constraints. Multiple ratings are typically used, one for normal conditions and a higher rating for emergencies. The primary means of limiting the flow of power on transmission lines is to adjust selectively the output of generators.

4. **Keep the system in a stable condition.** Because the electric system is interconnected and dynamic, electrical stability limits must be observed. Stability problems can develop very quickly—in just a few cycles (a cycle is 1/60th of a second)—or more slowly, over seconds or minutes. The main concern is to ensure that generation dispatch and the resulting power flows and voltages are such that the system is stable at all times. (As will be described later in this report, part of the Eastern Interconnection became unstable on August 14, resulting in a cascading outage over a wide area.) Stability limits, like thermal limits, are expressed as a maximum amount of electricity that can be safely transferred over transmission lines.

   There are two types of stability limits: (1) Voltage stability limits are set to ensure that the unplanned loss of a line or generator (which may have been providing locally critical reactive power support, as described previously) will not cause voltages to fall to dangerously low levels. If voltage falls too low, it begins to collapse uncontrollably, at which point automatic relays either shed load or trip generators to avoid damage. (2) Power (angle) stability limits are set to ensure that a short circuit or an unplanned loss of a line, transformer, or generator will not cause the remaining generators and loads being served to lose synchronism with one another. (Recall that all generators and loads within an interconnection must operate at or very near a common 60 Hz frequency.) Loss of synchronism with the common frequency means generators are operating out-of-step with one another. Even modest losses of synchronism can result in damage to generation equipment. Under extreme losses of synchronism, the grid may break apart into separate electrical islands; each island would begin to maintain its own frequency, determined by the load/generation balance within the island.

5. **Operate the system so that it remains in a reliable condition even if a contingency occurs, such as the loss of a key generator or transmission facility (the "N minus 1 criterion").** The central organizing principle of electricity reliability management is to plan for the unexpected. The unique features of electricity mean

that problems, when they arise, can spread and escalate very quickly if proper safeguards are not in place. Accordingly, through years of experience, the industry has developed a sequence of defensive strategies for maintaining reliability based on the assumption that equipment can and will fail unexpectedly upon occasion.

This principle is expressed by the requirement that the system must be operated at all times to ensure that it will remain in a secure condition (generally within emergency ratings for current and voltage and within established stability limits) following the loss of the most important generator or transmission facility (a "worst single contingency"). This is called the "N-1 criterion." In other words, because a generator or line trip can occur at any time from random failure, the power system must be operated in a preventive mode so that the loss of the most important generator or transmission facility does not jeopardize the remaining facilities in the system by causing them to exceed their emergency ratings or stability limits, which could lead to a cascading outage.

Further, when a contingency does occur, the operators are required to identify and assess immediately the new worst contingencies, given the changed conditions, and promptly make any adjustments needed to ensure that if one of them were to occur, the system would still remain operational and safe. NERC operating policy requires that the system be restored as soon as practical but within no more than 30 minutes to compliance with normal limits, and to a condition where it can once again withstand the next-worst single contingency without violating thermal, voltage, or stability limits. A few areas of the grid are operated to withstand the concurrent loss of two or more facilities (i.e., "N-2"). This may be done, for example, as an added safety measure to protect a densely populated metropolitan area or when lines share a common structure and could be affected by a common failure mode, e.g., a single lightning strike.

6. **Plan, design, and maintain the system to operate reliably.** Reliable power system operation requires far more than monitoring and controlling the system in real-time. Thorough planning, design, maintenance, and analysis are required to ensure that the system can be operated reliably and within safe limits. Short-term planning addresses day-ahead and week-ahead operations planning; long-term planning focuses on providing adequate generation resources and transmission capacity to ensure that in the future the system will be able to withstand severe contingencies without experiencing widespread, uncontrolled cascading outages.

   A utility that serves retail customers must estimate future loads and, in some cases, arrange for adequate sources of supplies and plan adequate transmission and distribution infrastructure. NERC planning standards identify a range of possible contingencies and set corresponding expectations for system performance under several categories of possible events. Three categories represent the more probable types of events that the system must be planned to withstand. A fourth category represents "extreme events" that may involve substantial loss of customer load and generation in a widespread area. NERC planning standards also address requirements for voltage support and reactive power, disturbance monitoring, facility ratings, system modeling and data requirements, system protection and control, and system restoration.

7. **Prepare for emergencies.** System operators are required to take the steps described above to plan and operate a reliable power system, but emergencies can still occur because of external factors such as severe weather, operator error, or equipment failures that exceed planning, design, or operating criteria. For these rare events, the operating entity is required to have emergency procedures covering a credible range of emergency scenarios. Operators must be trained to recognize and take effective action in response to these emergencies. To deal with a system emergency that results in a blackout, such as the one that occurred on August 14, 2003, there must be procedures and capabilities to use "black start" generators (capable of restarting with no external power source) and to coordinate operations in order to restore the system as quickly as possible to a normal and reliable condition.

Reliability Organizations Oversee Grid Reliability in North America

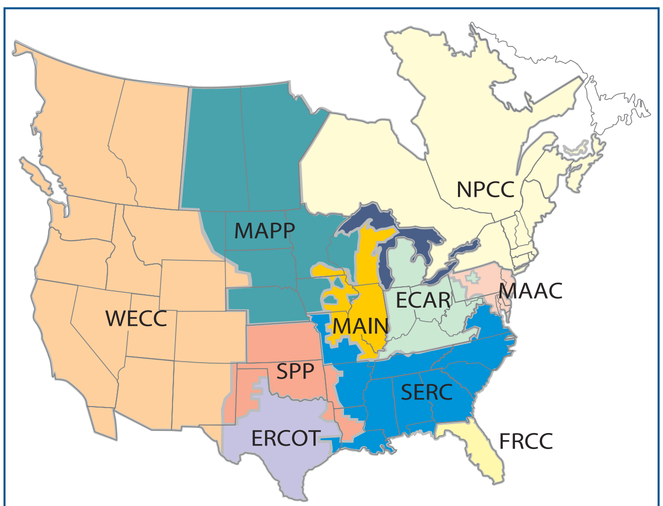
NERC is a non-governmental entity whose mission is to ensure that the bulk electric system in North America is reliable, adequate and secure.

The organization was established in 1968, as a result of the Northeast blackout in 1965. Since its inception, NERC has operated as a voluntary organization, relying on reciprocity, peer pressure and the mutual self-interest of all those involved to ensure compliance with reliability requirements. An independent board governs NERC.

To fulfill its mission, NERC:

- Sets standards for the reliable operation and planning of the bulk electric system.
- Monitors and assesses compliance with standards for bulk electric system reliability.
- Provides education and training resources to promote bulk electric system reliability.
- Assesses, analyzes and reports on bulk electric system adequacy and performance.
- Coordinates with Regional Reliability Councils and other organizations.
- Coordinates the provision of applications (tools), data and services necessary to support the reliable operation and planning of the bulk electric system.
- Certifies reliability service organizations and personnel.
- Coordinates critical infrastructure protection of the bulk electric system.
- Enables the reliable operation of the interconnected bulk electric system by facilitating information exchange and coordination among reliability service organizations.

Figure 2.5. NERC Regions



Recent changes in the electricity industry have altered many of the traditional mechanisms, incentives and responsibilities of the entities involved in ensuring reliability, to the point that the voluntary system of compliance with reliability standards is generally recognized as not adequate to current needs.[2] NERC and many other electricity organizations support the development of a new mandatory system of reliability standards and compliance, backstopped in the United States by the Federal Energy Regulatory Commission. This will require federal legislation in the United States to provide for the creation of a new electric reliability organization with the statutory authority to enforce compliance with reliability standards among all market participants. Appropriate government entities in Canada and Mexico are prepared to take similar action, and some have already done so. In the meantime, NERC encourages compliance with its reliability standards through an agreement with its members.

NERC's members are ten Regional Reliability Councils. (See Figure 2.5 for a map showing the locations and boundaries of the regional councils.) The regional councils and NERC have opened their membership to include all segments of the electric industry: investor-owned utilities; federal power agencies; rural electric cooperatives; state, municipal and provincial utilities; independent power producers; power marketers; and end-use customers. Collectively, the members of the NERC regions account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico. The ten regional councils jointly fund NERC and adapt NERC standards to meet the needs of their regions. The August 14 blackout affected three NERC regional reliability councils—East Central Area Reliability Coordination Agreement (ECAR), Mid-Atlantic Area Council (MAAC), and Northeast Power Coordinating Council (NPCC).

"Control areas" are the primary operational entities that are subject to NERC and regional council standards for reliability. A control area is a geographic area within which a single entity, Independent System Operator (ISO), or Regional Transmission Organization (RTO) balances generation and loads in real time to maintain reliable operation. Control areas are linked with each other through transmission interconnection tie lines. Control area operators control generation directly to maintain their electricity interchange schedules with other control areas. They also operate collectively to support the reliability of

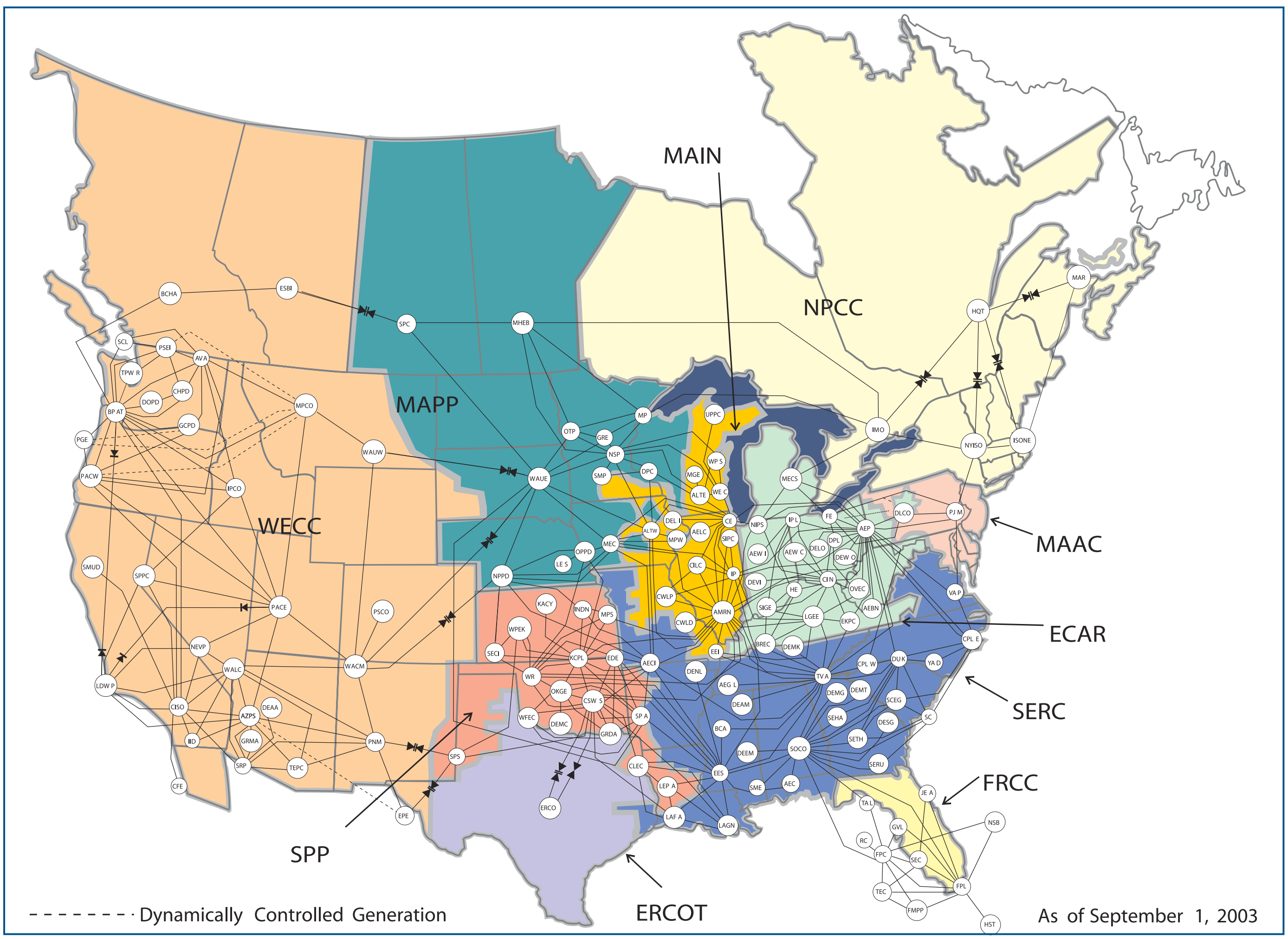
their interconnection. As shown in Figure 2.6, there are approximately 140 control areas in North America. The control area dispatch centers have sophisticated monitoring and control systems and are staffed 24 hours per day, 365 days per year.

Traditionally, control areas were defined by utility service area boundaries and operations were largely managed by vertically integrated utilities that owned and operated generation, transmission, and distribution. While that is still true in some areas, there has been significant restructuring of operating functions and some consolidation of control areas into regional operating entities. Utility industry restructuring has led to an unbundling of generation, transmission and distribution activities such that the ownership and operation of these assets have been separated either functionally or through the formation of independent entities called Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs).

- ISOs and RTOs in the United States have been authorized by FERC to implement aspects of the Energy Policy Act of 1992 and subsequent FERC policy directives.
- The primary functions of ISOs and RTOs are to manage in real time and on a day-ahead basis the reliability of the bulk power system and the operation of wholesale electricity markets within their footprint.
- ISOs and RTOs do not own transmission assets; they operate or direct the operation of assets owned by their members.
- ISOs and RTOs may be control areas themselves, or they may encompass more than one control area.
- ISOs and RTOs may also be NERC Reliability Coordinators, as described below.

Five RTOs/ISOs are within the area directly affected by the August 14 blackout. They are:

Figure 2.6. NERC Regions and Control Areas



- Midwest Independent System Operator (MISO)
- PJM Interconnection (PJM)
- New York Independent System Operator (NYISO)
- New England Independent System Operator (ISO-NE)
- Ontario Independent Market Operator (IMO)

Reliability coordinators provide reliability oversight over a wide region. They prepare reliability assessments, provide a wide-area view of reliability, and coordinate emergency operations in real time for one or more control areas. They do not participate in the wholesale or retail market functions. There are currently 18 reliability coordinators in North America. Figure 2.7 shows the locations and boundaries of their respective areas.

Key Parties in the Pre-Cascade Phase of the August 14 Blackout

The initiating events of the blackout involved two control areas—FirstEnergy (FE) and American Electric Power (AEP)—and their respective reliability coordinators, MISO and PJM (see Figures 2.7 and 2.8). These organizations and their reliability responsibilities are described briefly in this final subsection.

1. **FirstEnergy operates a control area in northern Ohio.** FirstEnergy (FE) consists of seven electric utility operating companies. Four of these companies, Ohio Edison, Toledo Edison, The Illuminating Company, and Penn Power, operate in the NERC ECAR region, with MISO serving as their reliability coordinator. These four companies now operate as one integrated control area managed by FE.[3]

2. **American Electric Power (AEP) operates a control area in Ohio just south of FE.** AEP is both a transmission operator and a control area operator.

3. **Midwest Independent System Operator (MISO) is the reliability coordinator for FirstEnergy.** The Midwest Independent System Operator (MISO) is the reliability coordinator for a region of more than one million square miles, stretching from Manitoba, Canada in the north to Kentucky in the south, from Montana in the west to western Pennsylvania in the east. Reliability coordination is provided by two offices, one in Minnesota, and the other at the MISO headquarters in Indiana. Overall, MISO provides reliability coordination for 37 control areas, most of which are members of MISO.

4. **PJM is AEP's reliability coordinator.** PJM is one of the original ISOs formed after FERC orders 888 and 889, but was established as a regional power pool in 1935. PJM recently expanded its footprint to include control areas and transmission operators within MAIN and ECAR (PJM-West). It performs its duties as a reliability coordinator in different ways, depending on the control areas involved. For PJM-East, it is both the control area and reliability coordinator for ten utilities, whose transmission systems span the Mid-Atlantic region of New Jersey, most of Pennsylvania, Delaware, Maryland, West Virginia, Ohio, Virginia, and the District of Columbia. The PJM-West facility has the reliability coordinator desk for five control areas (AEP, Commonwealth Edison, Duquesne Light,

Figure 2.7. NERC Reliability Coordinators

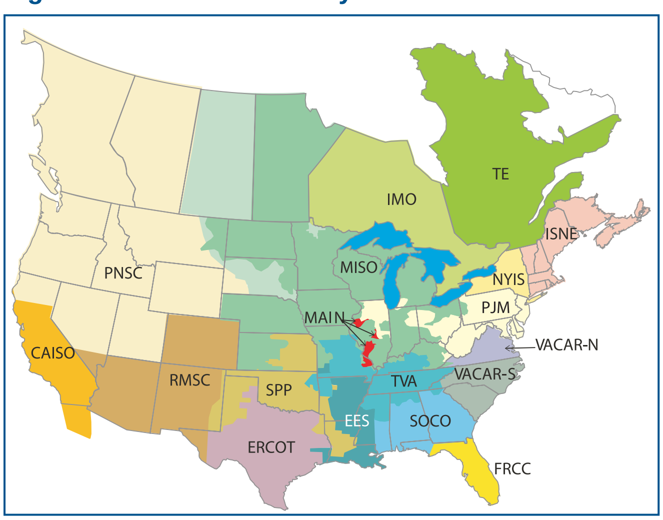
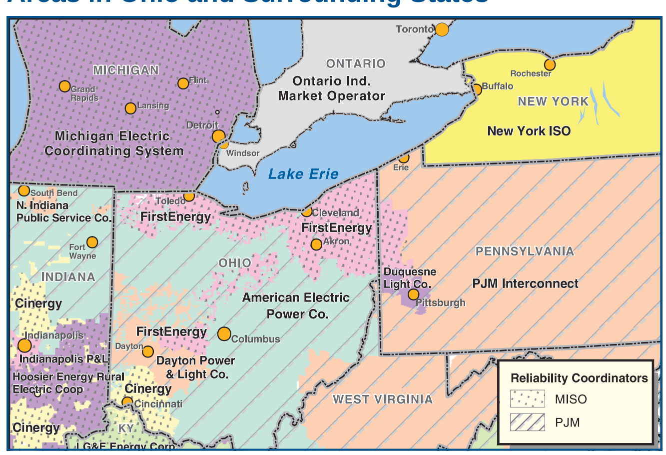


Figure 2.8. Reliability Coordinators and Control Areas in Ohio and Surrounding States



Dayton Power and Light, and Ohio Valley Electric Cooperative) and three generation-only control areas (Duke Energy's Washington County (Ohio) facility, Duke's Lawrence County/Hanging Rock (Ohio) facility, and Allegheny Energy's Buchanan (West Virginia) facility.

Reliability Responsibilities of Control Area Operators and Reliability Coordinators

1. **Control area operators have primary responsibility for reliability.** Their most important responsibilities, in the context of this report, are:

   N-1 criterion. NERC Operating Policy 2.A—Transmission Operations:

   "All CONTROL AREAS shall operate so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single contingency."

   Emergency preparedness and emergency response. NERC Operating Policy 5—Emergency Operations, General Criteria:

   "Each system and CONTROL AREA shall promptly take appropriate action to relieve any abnormal conditions, which jeopardize reliable Interconnection operation."

   "Each system, CONTROL AREA, and Region shall establish a program of manual and automatic load shedding which is designed to arrest frequency or voltage decays that could result in an uncontrolled failure of components of the interconnection."

Institutional Complexities and Reliability in the Midwest

The institutional arrangements for reliability in the Midwest are much more complex than they are in the Northeast-the areas covered by the Northeast Power Coordinating Council (NPCC) and the Mid-Atlantic Area Council (MAAC). There are two principal reasons for this complexity. One is that in NPCC and MAAC, the independent system operator (ISO) also serves as the single control area operator for the individual member systems. In comparison, MISO provides reliability coordination for 35 control areas in the ECAR, MAIN, and MAPP regions and 2 others in the SPP region, and PJM provides reliability coordination for 8 control areas in the ECAR and MAIN regions (plus one in MAAC). (See table below.) This results in 18 control-area-to-control-area interfaces across the PJM/MISO reliability coordinator boundary.

The other is that MISO has less reliability-related authority over its control area members than PJM has over its members. Arguably, this lack of authority makes day-to-day reliability operations more challenging. Note, however, that (1) FERC's authority to require that MISO have greater authority over its members is limited; and (2) before approving MISO, FERC asked NERC for a formal assessment of whether reliability could be maintained under the arrangements proposed by MISO and PJM. After reviewing proposed plans for reliability coordination within and between PJM and MISO, NERC replied affirmatively but provisionally. NERC conducted audits in November and December 2002 of the MISO and PJM reliability plans, and some of the recommendations of the audit teams are still being addressed. The adequacy of the plans and whether the plans were being implemented as written are factors in the NERC's ongoing investigation.

Reliability Coordinator (RC)	Control Areas in RC Area	Regional Reliability Councils Affected and Number of Control Areas	Control Areas of Interest in RC Area
MISO	37	ECAR (12), MAIN (9), MAPP (14), SPP (2)	FE, Cinergy, Michigan Electric Coordinated System
PJM	9	MAAC (1), ECAR (7), MAIN (1)	PJM, AEP, Dayton Power & Light
ISO New England	2	NPCC (2)	ISONE, Maritimes
New York ISO	1	NPCC (1)	NYISO
Ontario Independent Market Operator	1	NPCC (1)	IMO
Trans-Energie	1	NPCC (1)	Hydro Québec

NERC Operating Policy 5.A—Coordination with Other Systems:

"A system, CONTROL AREA, or pool that is experiencing or anticipating an operating emergency shall communicate its current and future status to neighboring systems, CONTROL AREAS, or pools and throughout the interconnection…. A system shall inform other systems … whenever … the system's condition is burdening other systems or reducing the reliability of the Interconnection …. [or whenever] the system's line loadings and voltage/reactive levels are such that a single contingency could threaten the reliability of the Interconnection."

NERC Operating Policy 5.C—Transmission System Relief:

"Action to correct an OPERATING SECURITY LIMIT violation shall not impose unacceptable stress on internal generation or transmission equipment, reduce system reliability beyond acceptable limits, or unduly impose voltage or reactive burdens on neighboring systems. If all other means fail, corrective action may require load reduction."

Operating personnel and training: NERC Operating Policy 8.B—Training:

"Each OPERATING AUTHORITY should periodically practice simulated emergencies. The scenarios included in practice situations should represent a variety of operating conditions and emergencies."

2. **Reliability Coordinators** such as MISO and PJM are expected to comply with all aspects of NERC Operating Policies, especially Policy 9, Reliability Coordinator Procedures, and its appendices. Key requirements include:

NERC Operating Policy 9, Criteria for Reliability Coordinators, 5.2:

Have "detailed monitoring capability of the RELIABILITY AREA and sufficient monitoring capability of the surrounding RELIABILITY AREAS to ensure potential security violations are identified."

NERC Operating Policy 9, Functions of Reliability Coordinators, 1.7:

"Monitor the parameters that may have significant impacts within the RELIABILITY AREA and with neighboring RELIABILITY AREAS with respect to … sharing with other RELIABILITY COORDINATORS any information regarding potential, expected, or actual critical operating conditions that could negatively impact other RELIABILITY AREAS. The RELIABILITY COORDINATOR will coordinate with other RELIABILITY COORDINATORS and CONTROL AREAS as needed to develop appropriate plans to mitigate negative impacts of potential, expected, or actual critical operating conditions…."

NERC Operating Policy 9, Functions of Reliability Coordinators, 6:

"Conduct security assessment and monitoring programs to assess contingency situations. Assessments shall be made in real time and for the operations planning horizon at the CONTROL AREA level with any identified problems reported to the RELIABILITY COORDINATOR. The RELIABILITY COORDINATOR is to ensure that CONTROL AREA, RELIABILITY AREA, and regional boundaries are sufficiently modeled to capture any problems crossing such boundaries."

What Constitutes an Operating Emergency?

An operating emergency is an unsustainable condition that cannot be resolved using the resources normally available. The NERC Operating Manual defines a "capacity emergency" as when a system's or pool's operating generation capacity, plus firm purchases from other systems, to the extent available or limited by transfer capability, is inadequate to meet its demand plus its regulating requirements. It defines an "energy emergency" as when a load-serving entity has exhausted all other options and can no longer provide its customers' expected energy requirements. A transmission emergency exists when "the system's line loadings and voltage/ reactive levels are such that a single contingency could threaten the reliability of the Interconnection." Control room operators and dispatchers are given substantial latitude to determine when to declare an emergency. (See page 42 in Chapter 4 for more detail.)

Endnotes

[1] The province of Quebec, although considered a part of the Eastern Interconnection, is connected to the rest of the Eastern Interconnection primarily by DC ties. In this instance, the DC ties acted as buffers between portions of the Eastern Interconnection; transient disturbances propagate through them less readily. Therefore, the electricity system in Quebec was not affected by the outage, except for a small portion of the

province's load that is directly connected to Ontario by AC transmission lines. (Although DC ties can act as a buffer between systems, the tradeoff is that they do not allow instantaneous generation support following the unanticipated loss of a generating unit.)

[2] See, for example, *Maintaining Reliability in a Competitive Electric Industry* (1998), a report to the U.S. Secretary of Energy by the Task Force on Electric Systems Reliability; *National Energy Policy* (2001), a report to the President of the United States by the National Energy Policy Development Group, p. 7-6; and *National Transmission Grid Study* (2002), U.S. Dept. of Energy, pp. 46-48.

[3] The remaining three FE companies, Penelec, Met-Ed, and Jersey Central Power & Light, are in the NERC MAAC region and have PJM as their reliability coordinator. The focus of this report is on the portion of FE in ECAR reliability region and within the MISO reliability coordinator footprint.

3. Status of the Northeastern Power Grid Before the Blackout Sequence Began

Summary

This chapter reviews the state of the northeast portion of the Eastern Interconnection during the days prior to August 14, 2003 and up to 15:05 EDT on August 14 to determine whether conditions at that time were in some way unusual and might have contributed to the initiation of the blackout. The Task Force's investigators found that at 15:05 EDT, immediately before the tripping (automatic shutdown) of FirstEnergy's (FE) Harding-Chamberlin 345-kV transmission line, the system was able to be operated reliably following the occurrence of any of more than 800 contingencies, including the loss of the Harding-Chamberlin line. At that point the system was being operated near (but still within) prescribed limits and in compliance with NERC's operating policies.

Determining that the system was in a reliable operational state at that time is extremely significant for understanding the causes of the blackout. It means that none of the electrical conditions on the system before 15:05 EDT was a direct cause of the blackout. This eliminates a number of possible causes of the blackout, whether individually or in combination with one another, such as:

- High power flows to Canada
- System frequency variations
- Low voltages earlier in the day or on prior days
- Low reactive power output from IPPs
- Unavailability of individual generators or transmission lines.

It is important to emphasize that establishing whether conditions were normal or unusual prior to and on August 14 has no direct bearing on the responsibilities and actions expected of the organizations and operators who are charged with ensuring power system reliability. As described in Chapter 2, the electricity industry has developed and codified a set of mutually reinforcing reliability standards and practices to ensure that system operators are prepared for the unexpected. The basic assumption underlying these standards and practices is that power system elements will fail or become unavailable in unpredictable ways. Sound reliability management is designed to ensure that safe operation of the system will continue following the unexpected loss of any key element (such as a major generator or key transmission facility). These practices have been designed to maintain a functional and reliable grid, regardless of whether actual operating conditions are normal. It is a basic principle of reliability management that "operators must operate the system they have in front of them"—unconditionally.

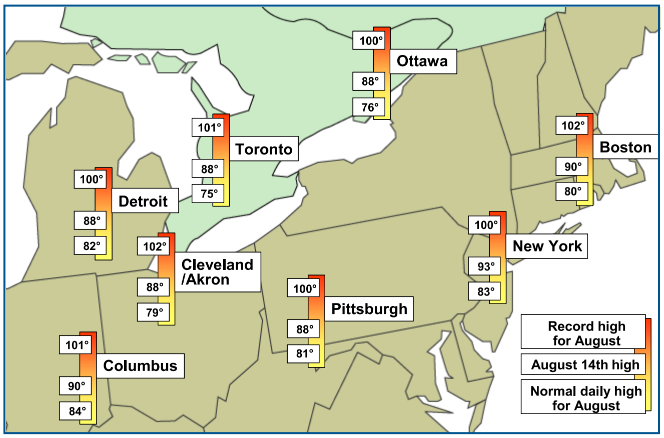
In terms of day-ahead planning, this means evaluating and if necessary adjusting the planned generation pattern (scheduled electricity transactions) to change the transmission flows, so that if a key facility were lost, the operators would still be able to readjust the remaining system and operate within safe limits. In terms of real-time operations, this means that the system should be operated at all times so as to be able to withstand the loss of any single facility and still remain within the system's thermal, voltage, and stability limits. If a facility is lost unexpectedly, the system operators must determine whether to make operational changes to ensure that the remaining system is able to withstand the loss of yet another key element and still remain able to operate within safe limits. This includes adjusting generator outputs, curtailing electricity transactions, and if necessary, shedding interruptible and firm customer load—i.e., cutting some customers off temporarily, and in the right locations, to reduce electricity demand to a level that matches what the system is then able to deliver safely.

Electric Demands on August 14

Temperatures on August 14 were above normal throughout the northeast region of the United

States and in eastern Canada. As a result, electricity demands were high due to high air conditioning loads typical of warm days in August, though not unusually so. System operators had successfully managed higher demands both earlier in the summer and in previous years. Recorded peak electric demands throughout the region on August 14 were below peak demands recorded earlier in the summer of 2003 (Figure 3.1).

Figure 3.1. August 2003 Temperatures in the U.S. Northeast and Eastern Canada



Power Flow Patterns

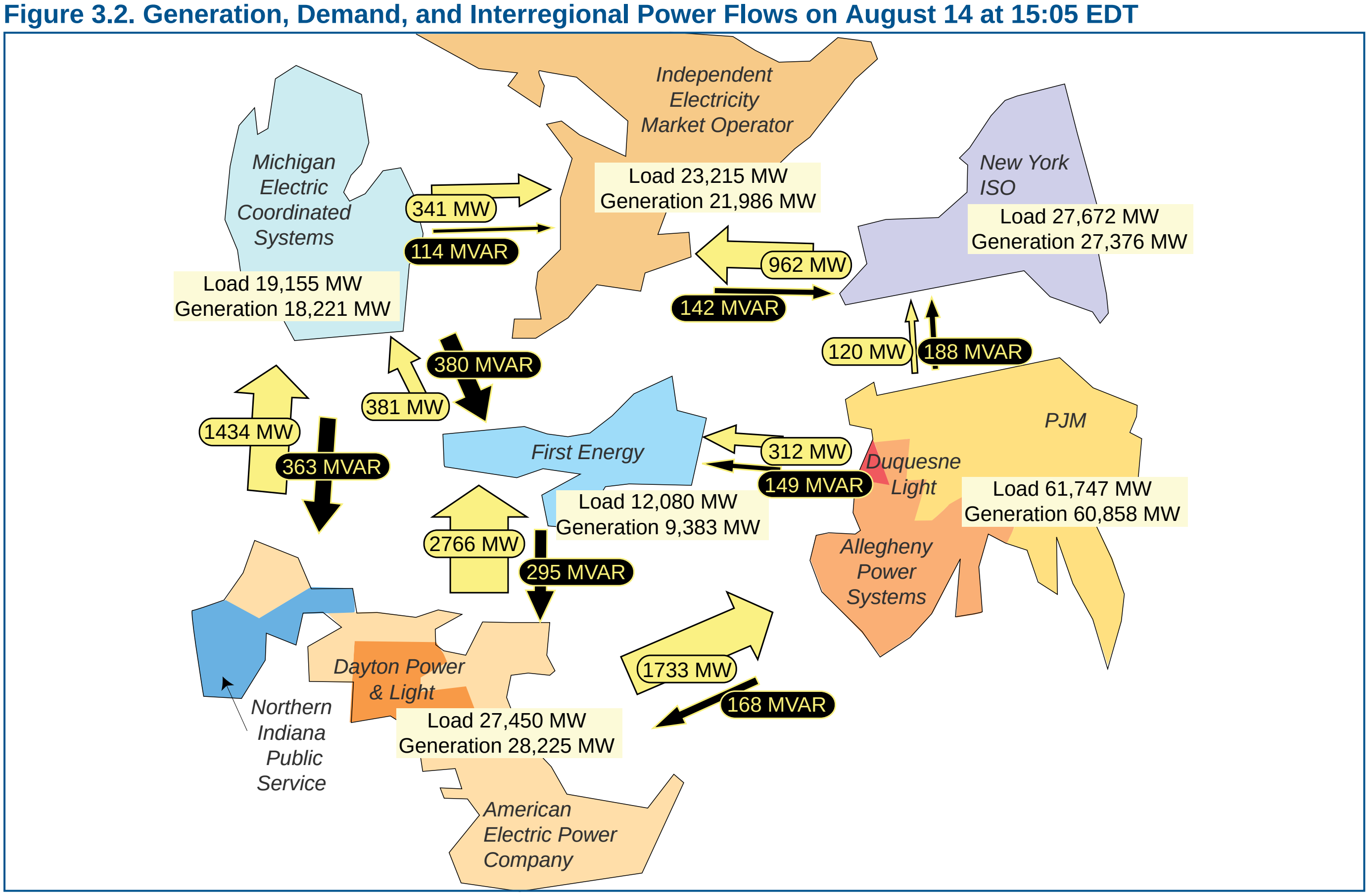
On August 14, the flow of power through the ECAR region was heavy as a result of large transfers of power from the south (Tennessee, Kentucky, Missouri, etc.) and west (Wisconsin, Minnesota, Illinois, etc.) to the north (Ohio, Michigan, and Ontario) and east (New York). The destinations for much of the power were northern Ohio, Michigan, PJM, and Ontario (Figure 3.2).

While heavy, these transfers were not beyond previous levels or in directions not seen before (Figure 3.3). The level of imports into Ontario on August 14 was high but not unusual, and well within IMO's import capability. Ontario's IMO is a frequent importer of power, depending on the availability and price of generation within Ontario. IMO had imported similar and higher amounts of power several times during the summers of 2002 and 2003.

System Frequency

Although system frequency on the Eastern Interconnection was somewhat more variable on

Figure 3.2. Generation, Demand, and Interregional Power Flows on August 14 at 15:05 EDT



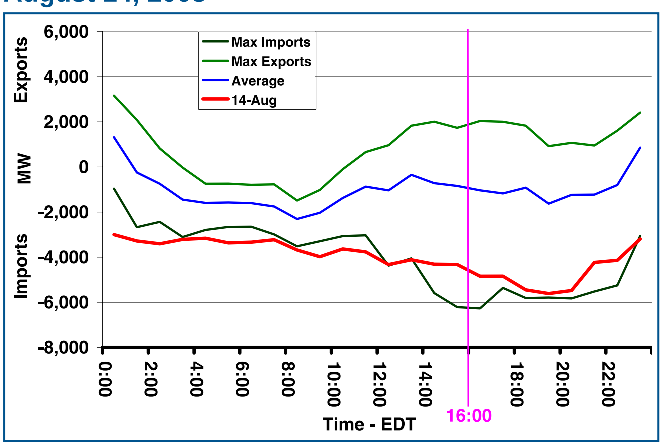
August 14 prior to 15:05 EDT compared with recent history, it was well within the bounds of safe operating practices as outlined in NERC operating policies. As a result, system frequency variation was not a cause of the initiation of the blackout. But once the cascade was initiated, the large frequency swings that were induced became a principal means by which the blackout spread across a wide area (Figure 3.4).

Assuming stable conditions, the system frequency is the same across an interconnected grid at any particular moment. System frequency will vary from moment to moment, however, depending on the second-to-second balance between aggregate generation and aggregate demand across the interconnection. System frequency is monitored on a continuous basis.

Frequency Management

Each control area is responsible for maintaining a balance between its generation and demand. If persistent under-frequency occurs, at least one control area somewhere is "leaning on the grid," meaning that it is taking unscheduled electricity from the grid, which both depresses system frequency and creates unscheduled power flows. In practice, minor deviations at the control area level are routine; it is very difficult to maintain an exact balance between generation and demand. Accordingly, NERC has established operating rules that specify maximum permissible deviations, and focus on prohibiting persistent deviations, but not instantaneous ones. NERC monitors the performance of control areas through specific measures of control performance that gauge how accurately each control area matches its load and generation.

Figure 3.3. Northeast Central Area Scheduled Imports and Exports: Summer 2003 Compared to August 14, 2003



Note: Area covered includes ECAR, PJM, Ontario, and New York, without imports from the Maritime Provinces, ISO-New England, or Hydro-Quebec.

Generation Facilities Unavailable on August 14

Several key generators in the region were out of service going into the day of August 14. On any given day, some generation and transmission capacity is unavailable; some facilities are out for routine maintenance, and others have been forced out by an unanticipated breakdown and require repairs. August 14, 2003, was no exception (Table 3.1).

The generating units that were not available on August 14 provide real and reactive power directly to the Cleveland, Toledo, and Detroit areas. Under standard practice, system operators take into account the unavailability of such units and any

Figure 3.4. Frequency on August 14, 2003, up to 15:31 EDT

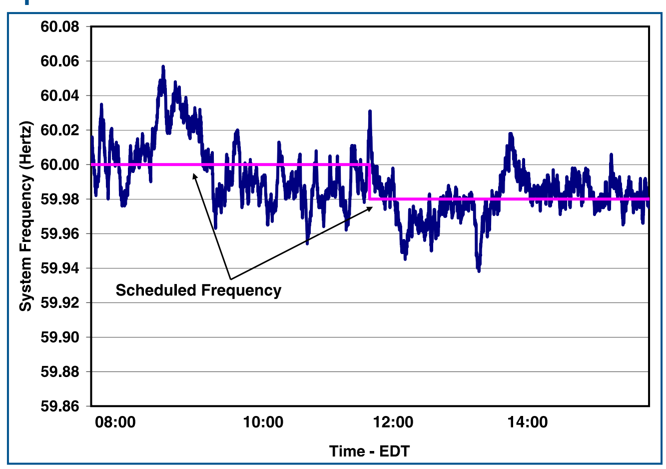


Table 3.1. Generators Not Available on August 14

Generator	Rating	Reason
Davis-Besse Nuclear Unit	750 MW	Prolonged NRC-ordered outage beginning on 3/22/02
Eastlake Unit 4	238 MW	Forced outage on 8/13/03
Monroe Unit 1	817 MW	Planned outage, taken out of service on 8/8/03
Cook Nuclear Unit 2	1,060 MW	Outage began on 8/13/03

transmission facilities known to be out of service in the day-ahead planning studies they perform to determine the condition of the system for the next day. Knowing the status of key facilities also helps operators determine in advance the safe electricity transfer levels for the coming day.

MISO's day-ahead planning studies for August 14 took these generator outages and known transmission outages into account and determined that the regional system could still be operated safely. The unavailability of these generation units and transmission facilities did not cause the blackout.

Voltages

During the days before August 14 and throughout the morning and mid-day on August 14, voltages were depressed in a variety of locations in northern Ohio because of high air conditioning demand and other loads, and power transfers into and across the region. (Unlike frequency, which is constant across the interconnection, voltage varies by location, and operators monitor voltages continuously at key locations across their systems.) However, actual measured voltage levels at key points on FE's transmission system on the morning of August 14 and up to 15:05 EDT were within the range previously specified by FE as acceptable. Note, however, that many control areas in the Eastern Interconnection have set their acceptable voltage bands at levels higher than that used by FE. For example, AEP's minimum acceptable voltage level is 95% of a line's nominal rating, as compared to FE's 92%.[1]

Voltage management is especially challenging on hot summer days because of high air conditioning requirements, other electricity demand, and high transfers of power for economic reasons, all of which increase the need for reactive power. Operators address these challenges through long-term planning, day-ahead planning, and real-time adjustments to operating equipment. On August 14, for example, PJM implemented routine voltage management procedures developed for heavy load conditions. FE also began preparations early in the afternoon of August 14, requesting capacitors to be restored to service[2] and additional voltage support from generators.[3] Such actions were typical of many system operators that day as well as on other days with high electric demand. As the day progressed, operators across the region took additional actions, such as increasing plants' reactive power output, plant redispatch, transformer tap changes, and increased use of capacitors to respond to changing voltage conditions.

The power flow data for northern Ohio on August 14 just before the Harding-Chamberlin line tripped at 15:05 EDT (Figure 3.2) show that FE's load was approximately 12,080 MW. FE was importing about 2,575 MW, 21% of its total system needs, and generating the remainder. With this high level of imports and high air conditioning loads in the

Independent Power Producers and Reactive Power

Independent power producers (IPPs) are power plants that are not owned by utilities. They operate according to market opportunities and their contractual agreements with utilities, and may or may not be under the direct control of grid operators. An IPP's reactive power obligations are determined by the terms of its contractual interconnection agreement with the local transmission owner. Under routine conditions, some IPPs provide limited reactive power because they are not required or paid to produce it; they are only paid to produce active power. (Generation of reactive power by a generator can require scaling back generation of active power.) Some contracts, however, compensate IPPs for following a voltage schedule set by the system operator, which requires the IPP to vary its output of reactive power as system conditions change. Further, contracts typically require increased reactive power production from IPPs when it is requested by the control area operator during times of a system emergency. In some contracts, provisions call for the payment of opportunity costs to IPPs when they are called on for reactive power (i.e., they are paid the value of foregone active power production).

Thus, the suggestion that IPPs may have contributed to the difficulties of reliability management on August 14 because they don't provide reactive power is misplaced. What the IPP is required to produce is governed by contractual arrangements, which usually include provisions for contributions to reliability, particularly during system emergencies. More importantly, it is the responsibility of system planners and operators, not IPPs, to plan for reactive power requirements and make any short-term arrangements needed to ensure that adequate reactive power resources will be available.

metropolitan areas around the southern end of Lake Erie, FE's system reactive power needs rose further. Investigation team modeling indicates that at 15:00 EDT, with Eastlake 5 out of service, FE was a net importer of about 132 MVAr. A significant amount of power also was flowing through northern Ohio on its way to Michigan and Ontario (Figure 3.2). The net effect of this flow pattern and load composition was to depress voltages in northern Ohio.

Unanticipated Outages of Transmission and Generation on August 14

Three significant unplanned outages occurred in the Ohio area on August 14 prior to 15:05 EDT. Around noon, several Cinergy transmission lines in south-central Indiana tripped; at 13:31 EDT, FE's Eastlake 5 generating unit along the southwestern shore of Lake Erie tripped; at 14:02 EDT, a Dayton Power and Light (DPL) line, the Stuart-Atlanta 345-kV line in southern Ohio, tripped.

- Transmission lines on the Cinergy 345-, 230-, and 138-kV systems experienced a series of outages starting at 12:08 EDT and remained out of service during the entire blackout. The loss of these lines caused significant voltage and loading problems in the Cinergy area. Cinergy made generation changes, and MISO operators responded by implementing transmission load relief (TLR) procedures to control flows on the transmission system in south-central Indiana. System modeling by the investigation team (see details below, page 20) showed that the loss of these lines was *not* electrically related to subsequent events in northern Ohio that led to the blackout.
- The DPL Stuart-Atlanta 345-kV line, linking DPL to AEP and monitored by the PJM reliability coordinator, tripped at 14:02 EDT. This was the result of a tree contact, and the line remained out of service during the entire blackout. As explained below, system modeling by the investigation team has shown that this outage was not a cause of the subsequent events in northern Ohio that led to the blackout. However, since the line was not in MISO's footprint, MISO operators did not monitor the status of this line, and did not know that it had gone out of service. This led to a data mismatch that prevented MISO's state estimator (a key monitoring tool) from producing usable results later in the day at a time when system conditions in FE's control area were deteriorating (see details below, page 27).
- Eastlake Unit 5 is a 597-MW generating unit located just west of Cleveland near Lake Erie. It is a major source of reactive power support for the Cleveland area. It tripped at 13:31. The cause of the trip was that as the Eastlake 5 operator sought to increase the unit's reactive power

Power Flow Simulation of Pre-Cascade Conditions

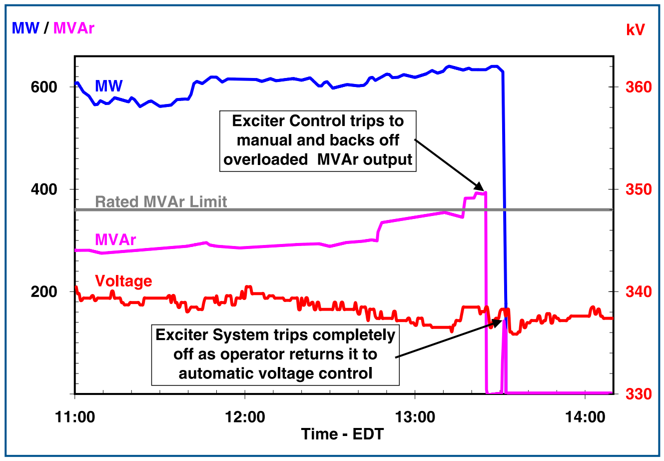
The bulk power system has no memory. It does not matter if frequencies or voltage were unusual an hour, a day, or a month earlier. What matters for reliability are loadings on facilities, voltages, and system frequency at a given moment and the collective capability of these system components at that same moment to withstand a contingency without exceeding thermal, voltage, or stability limits.

Power system engineers use a technique called power flow simulation to reproduce known operating conditions at a specific time by calibrating an initial simulation to observed voltages and line flows. The calibrated simulation can then be used to answer a series of "what if" questions to determine whether the system was in a safe operating state at that time. The "what if" questions consist of systematically simulating outages by removing key elements (e.g., generators or transmission lines) one by one and reassessing the system each time to determine whether line or voltage limits would be exceeded. If a limit is exceeded, the system is not in a secure state. As described in Chapter 2, NERC operating policies require operators, upon finding that their system is not in a reliable state, to take immediate actions to restore the system to a reliable state as soon as possible and within a maximum of 30 minutes.

To analyze the evolution of the system on the afternoon of August 14, this process was followed to model several points in time, corresponding to key transmission line trips. For each point, three solutions were obtained: (1) conditions immediately before a facility tripped off; (2) conditions immediately after the trip; and (3) conditions created by any automatic actions taken following the trip.

output (Figure 3.5), the unit's protection system detected a failure and tripped the unit off-line. The loss of the Eastlake 5 unit did not put the grid into an unreliable state—i.e., it was still able to withstand safely another contingency. However, the loss of the unit required FE to import additional power to make up for the loss of the unit's output (540 MW), made voltage management in northern Ohio more challenging, and gave FE operators less flexibility in operating their system (see details below, page 27).

Figure 3.5. MW and MVAr Output from Eastlake Unit 5 on August 14



Model-Based Analysis of the State of the Regional Power System at 15:05 EDT, Before the Loss of FE's Harding-Chamberlin 345-kV Line

As the first step in modeling the evolution of the August 14 blackout, the investigative team established a base case by creating a power flow simulation for the entire Eastern Interconnection and benchmarking it to recorded system conditions at 15:05 EDT on August 14. The team started with a projected summer 2003 power flow case developed in the spring of 2003 by the Regional Reliability Councils to establish guidelines for safe operations for the coming summer. The level of detail involved in this region-wide study far exceeds that normally considered by individual control areas and reliability coordinators. It consists of a detailed representation of more than 43,000 buses (points at which lines, transformers, and/or generators converge), 57,600 transmission lines, and all major generating stations across the northern U.S. and eastern Canada. The team then revised the summer power flow case to match recorded generation, demand, and power interchange levels among control areas at 15:05 EDT on August 14. The benchmarking consisted of matching the calculated voltages and line flows to recorded observations at more than 1,500 locations within the grid. Thousands of hours of effort were required to benchmark the model satisfactorily to observed conditions at 15:05 EDT.

Once the base case was benchmarked, the team ran a contingency analysis that considered more than 800 possible events as points of departure from the 15:05 EDT case. None of these contingencies resulted in a violation of a transmission line loading or bus voltage limit prior to the trip of FE's Harding-Chamberlin 345-kV line. That is, according to these simulations, the system at 15:05 EDT was able to be operated safely following the occurrence of any of the tested contingencies. From an electrical standpoint, therefore, the Eastern Interconnection was then being operated within all established limits and in full compliance with NERC's operating policies. However, after loss of the Harding-Chamberlin 345-kV line, the system would have exceeded emergency ratings on several lines for two of the contingencies studied. In other words, it would no longer be operating in compliance with NERC operating policies.

Conclusion

Determining that the system was in a reliable operational state at 15:05 EDT is extremely significant for understanding the causes of the blackout. It means that none of the electrical conditions on the system before 15:05 EDT was a cause of the blackout. This eliminates high power flows to Canada, unusual system frequencies, low voltages earlier in the day or on prior days, and the unavailability of individual generators or transmission lines, either individually or in combination with one another, as direct, principal or sole causes of the blackout.

Endnotes

[1] DOE/NERC fact-finding meeting, September 2003, statement by Mr. Steve Morgan (FE), PR0890803, lines 5-23.

[2] Transmission operator at FE requested the restoration of the Avon Substation capacitor bank #2. Example at Channel 3, 13:33:40.

[3] From 13:13 through 13:28, reliability operator at FE called nine plant operators to request additional voltage support. Examples at Channel 16, 13:13:18, 13:15:49, 13:16:44, 13:20:44, 13:22:07, 13:23:24, 13:24:38, 13:26:04, 13:28:40.

4. How and Why the Blackout Began

Summary

This chapter explains the major events—electrical, computer, and human—that occurred as the blackout evolved on August 14, 2003, and identifies the causes of the initiation of the blackout. It also lists initial findings concerning violations of NERC reliability standards. It presents facts collected by the investigation team and does not offer speculative or unconfirmed information or hypotheses. Some of the information presented here, such as the timing of specific electrical events, updates the Sequence of Events[1] released earlier by the Task Force.

The period covered in this chapter begins at 12:15 Eastern Daylight Time (EDT) on August 14, 2003 when inaccurate input data rendered MISO's state estimator (a system monitoring tool) ineffective. At 13:31 EDT, FE's Eastlake 5 generation unit tripped and shut down automatically. Shortly after 14:14 EDT, the alarm and logging system in FE's control room failed and was not restored until after the blackout. After 15:05 EDT, some of FE's 345-kV transmission lines began tripping out because the lines were contacting overgrown trees within the lines' right-of-way areas.

By around 15:46 EDT when FE, MISO and neighboring utilities had begun to realize that the FE system was in jeopardy, the only way that the blackout might have been averted would have been to drop at least 1,500 to 2,500 MW of load around Cleveland and Akron, and at this time the amount of load reduction required was increasing rapidly. No such effort was made, however, and by 15:46 EDT it may already have been too late regardless of any such effort. After 15:46 EDT, the loss of some of FE's key 345-kV lines in northern Ohio caused its underlying network of 138-kV lines to begin to fail, leading in turn to the loss of FE's Sammis-Star 345-kV line at 16:06 EDT. The chapter concludes with the loss of FE's Sammis-Star line, the event that triggered the uncontrollable cascade portion of the blackout sequence.

The loss of the Sammis-Star line triggered the cascade because it shut down the 345-kV path into northern Ohio from eastern Ohio. Although the area around Akron, Ohio was already blacked out due to earlier events, most of northern Ohio remained interconnected and electricity demand was high. This meant that the loss of the heavily overloaded Sammis-Star line instantly created major and unsustainable burdens on lines in adjacent areas, and the cascade spread rapidly as lines and generating units automatically took themselves out of service to avoid physical damage.

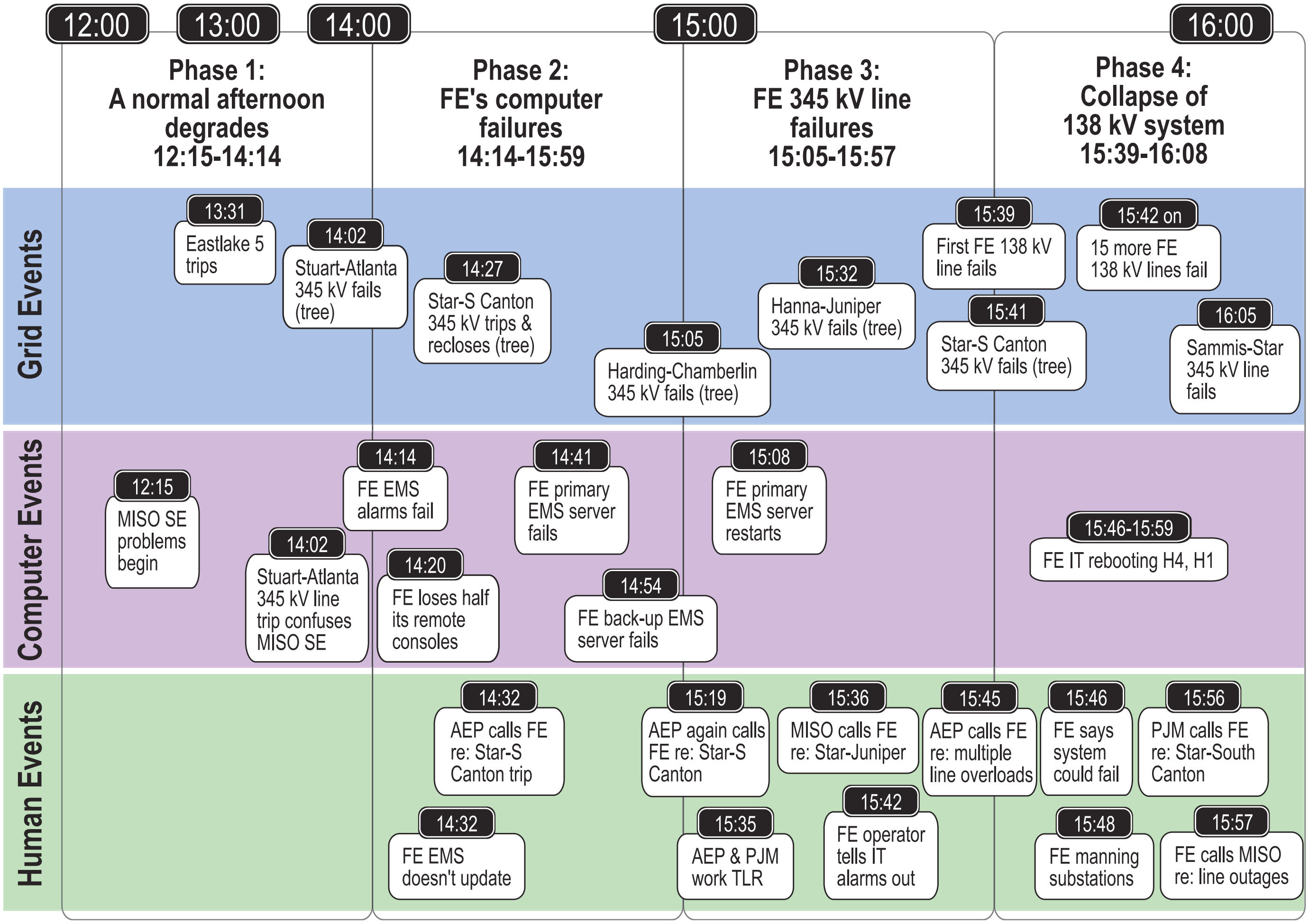
Chapter Organization

This chapter is divided into several phases that correlate to major changes within the FirstEnergy system and the surrounding area in the hours leading up to the cascade:

- **Phase 1:** A normal afternoon degrades
- **Phase 2:** FE's computer failures
- **Phase 3:** Three FE 345-kV transmission line failures and many phone calls
- **Phase 4:** The collapse of the FE 138-kV system and the loss of the Sammis-Star line

Key events within each phase are summarized in Figure 4.1, a timeline of major events in the origin of the blackout in Ohio. The discussion that follows highlights and explains these significant events within each phase and explains how the events were related to one another and to the cascade.

Figure 4.1. Timeline: Start of the Blackout in Ohio



Phase 1: A Normal Afternoon Degrades: 12:15 EDT to 14:14 EDT

Overview of This Phase

Northern Ohio was experiencing an ordinary August afternoon, with loads moderately high to serve air conditioning demand. FirstEnergy (FE) was importing approximately 2,000 MW into its service territory, causing its system to consume high levels of reactive power. With two of Cleveland's active and reactive power production anchors already shut down (Davis-Besse and Eastlake 4), the loss of the Eastlake 5 unit at 13:31 further depleted critical voltage support for the Cleveland-Akron area. Detailed simulation modeling reveals that the loss of Eastlake 5 was a significant factor in the outage later that afternoon—with Eastlake 5 gone, transmission line loadings were notably higher and after the loss of FE's Harding-Chamberlin line at 15:05, the system eventually became unable to sustain additional contingencies without line overloads above emergency ratings. Had Eastlake 5 remained in service, subsequent line loadings would have been lower and tripping due to tree contacts may not have occurred. Loss of Eastlake 5, however, did not initiate the blackout. Subsequent computer failures leading to the loss of situational awareness in FE's control room and the loss of key FE transmission lines due to contacts with trees were the most important causes.

At 14:02 EDT, Dayton Power & Light's (DPL) Stuart-Atlanta 345-kV line tripped off-line due to a tree contact. This line had no direct electrical effect on FE's system—but it did affect MISO's performance as reliability coordinator, even though PJM is the reliability coordinator for the DPL line. One of MISO's primary system condition evaluation tools, its state estimator, was unable to assess system conditions for most of the period between 12:37 EDT and 15:34 EDT, due to a combination of human error and the effect of the loss of DPL's

The Causes of the Blackout

The initiation of the August 14, 2003, blackout was caused by deficiencies in specific practices, equipment, and human decisions that coincided that afternoon. There were three groups of causes:

Group 1: Inadequate situational awareness at FirstEnergy Corporation (FE). In particular:

A) FE failed to ensure the security of its transmission system after significant unforeseen contingencies because it did not use an effective contingency analysis capability on a routine basis. (See page 28.)

B) FE lacked procedures to ensure that their operators were continually aware of the functional state of their critical monitoring tools. (See page 31.)

C) FE lacked procedures to test effectively the functional state of these tools after repairs were made. (See page 31.)

D) FE did not have additional monitoring tools for high-level visualization of the status of their transmission system to facilitate its operators' understanding of transmission system conditions after the failure of their primary monitoring/alarming systems. (See page 33.)

Group 2: FE failed to manage adequately tree growth in its transmission rights-of-way. This failure was the common cause of the outage of three FE 345-kV transmission lines. (See page 34.)

Group 3: Failure of the interconnected grid's reliability organizations to provide effective diagnostic support. In particular:

A) MISO did not have real-time data from Dayton Power and Light's Stuart-Atlanta 345-kV line incorporated into its state estimator (a system monitoring tool). This precluded MISO from becoming aware of FE's system problems earlier and providing diagnostic assistance to FE. (See page 24.)

B) MISO's reliability coordinators were using non-real-time data to support real-time "flowgate" monitoring. This prevented MISO from detecting an N-1 security violation in FE's system and from assisting FE in necessary relief actions. (See page 39.)

C) MISO lacked an effective means of identifying the location and significance of transmission line breaker operations reported by their Energy Management System (EMS). Such information would have enabled MISO operators to become aware earlier of important line outages. (See pages 27 and 36.)

D) PJM and MISO lacked joint procedures or guidelines on when and how to coordinate a security limit violation observed by one of them in the other's area due to a contingency near their common boundary. (See page 38.)

In the pages below, sections that relate to particular causes are denoted with the following symbols:

Cause 1: Inadequate Situational Awareness

Cause 2: Inadequate Tree Trimming

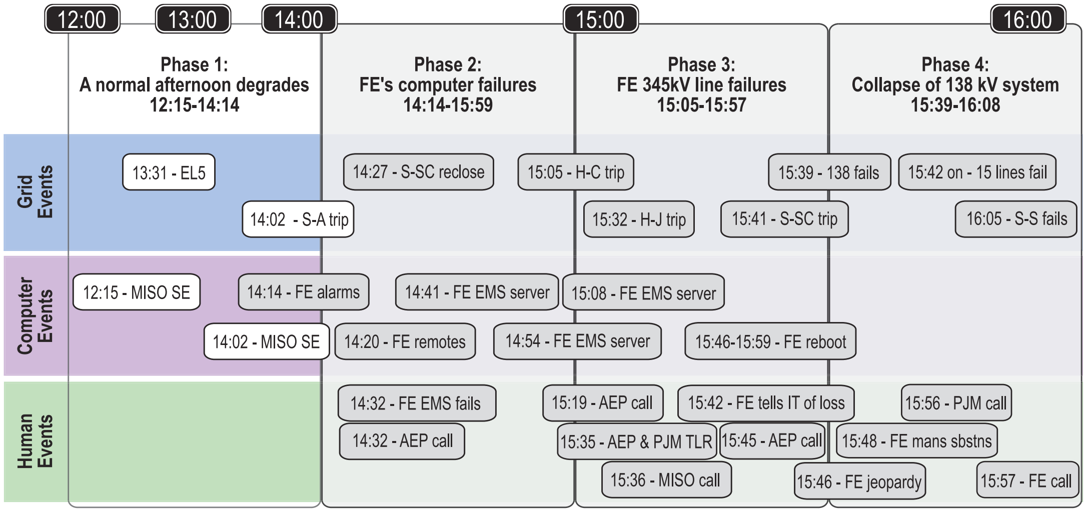
Cause 3: Inadequate RC Diagnostic Support

Stuart-Atlanta line on other MISO lines as reflected in the state estimator's calculations. Without an effective state estimator, MISO was unable to perform contingency analyses of generation and line losses within its reliability zone. Therefore, through 15:34 EDT MISO could not determine that with Eastlake 5 down, other transmission lines would overload if FE lost a major transmission line, and could not issue appropriate warnings and operational instructions.

In the investigation interviews, all utilities, control area operators, and reliability coordinators indicated that the morning of August 14 was a reasonably typical day. FE managers referred to it as peak load conditions on a less than peak load day.[2] Dispatchers consistently said that while voltages were low, they were consistent with historical voltages.[3] Throughout the morning and early afternoon of August 14, FE reported a growing need for voltage support in the upper Midwest.

The FE reliability operator was concerned about low voltage conditions on the FE system as early as 13:13 EDT. He asked for voltage support (i.e., increased reactive power output) from FE's

Figure 4.2. Timeline Phase 1



interconnected generators. Plants were operating in automatic voltage control mode (reacting to system voltage conditions and needs rather than constant reactive power output). As directed in FE's Manual of Operations,[4] the FE reliability operator began to call plant operators to ask for additional voltage support from their units. He noted to most of them that system voltages were sagging "all over." Several mentioned that they were already at or near their reactive output limits. None were asked to reduce their active power output to be able to produce more reactive output. He called the Sammis plant at 13:13 EDT, West Lorain at 13:15 EDT, Eastlake at 13:16 EDT, made three calls to unidentified plants between 13:20 EDT and 13:23 EDT, a "Unit 9" at 13:24 EDT, and two more at 13:26 EDT and 13:28 EDT.[5] The operators worked to get shunt capacitors at Avon that were out of service restored to support voltage.[6]

Following the loss of Eastlake 5 at 13:31 EDT, FE's operators' concern about voltage levels was heightened. They called Bayshore at 13:41 EDT and Perry at 13:43 EDT to ask the plants for more voltage support. Again, while there was substantial effort to support voltages in the Ohio area, First Energy personnel characterized the conditions as not being unusual for a peak load day, although this was not an all-time (or record) peak load day.

Key Phase 1 Events

1A) 12:15 EDT to 16:04 EDT: MISO's state estimator software solution was compromised, and MISO's single contingency reliability assessment became unavailable.

1B) 13:31:34 EDT: Eastlake Unit 5 generation tripped in northern Ohio.

1C) 14:02 EDT: Stuart-Atlanta 345-kV transmission line tripped in southern Ohio.

1A) MISO's State Estimator Was Turned Off: 12:15 EDT to 16:04 EDT

It is common for reliability coordinators and control areas to use a tool called a state estimator (SE) to improve the accuracy of the raw sampled data they have for the electric system by mathematically processing raw data to make it consistent with the electrical system model. The resulting information on equipment voltages and loadings is used in software tools such as real time contingency analysis (RTCA) to simulate various conditions and outages to evaluate the reliability of the power system. The RTCA tool is used to alert operators if the system is operating insecurely; it can be run either on a regular schedule (e.g., every 5 minutes), when triggered by some system event (e.g., the loss of a power plant or transmission line), or when initiated by an operator. MISO usually runs the SE every 5 minutes, and the RTCA less frequently. If the model does not have accurate and timely information about key pieces of system equipment or if key input data are wrong, the state estimator may be unable to reach a solution or it will reach a solution that is labeled as having a high degree of error. MISO considers its SE and RTCA tools to be still under development and not fully mature.

On August 14 at about 12:15 EDT, MISO's state estimator produced a solution with a high mismatch (outside the bounds of acceptable error). This was traced to an outage of Cinergy's

Initial Findings: Violations of NERC Reliability Standards

Note: These are initial findings and subject to further review by NERC. Additional violations may be identified.

Violation Number 1. Following the outage of the Chamberlin-Harding 345-kV line, FE did not take the necessary actions to return the system to a safe operating state within 30 minutes.[a]

Reference: NERC Operating Policy 2:

Following a contingency or other event that results in an OPERATING SECURITY LIMIT violation, the CONTROL AREA shall return its transmission system to within OPERATING SECURITY LIMITS soon as possible, but no longer than 30 minutes.

Violation Number 2. FE did not notify other systems of an impending system emergency.[b]

Reference: NERC Operating Policy 5:

Notifying other systems. A system shall inform other systems in their Region or subregion, through predetermined communication paths, whenever the following situations are anticipated or arise:

System is burdening others. The system's condition is burdening other systems or reducing the reliability of the Interconnection.

Lack of single contingency coverage. The system's line loadings and voltage/reactive levels are such that a single contingency could threaten the reliability of the Interconnection.

Violation Number 3. FE's state estimation/contingency analysis tools were not used to assess the system conditions.[c]

Reference: NERC Operating Policy 5:

Sufficient information and analysis tools shall be provided to the SYSTEM OPERATOR to determine the cause(s) of OPERATING SECURITY LIMIT violations. This information shall be provided in both real time and predictive formats so that the appropriate corrective actions may be taken.

Violation Number 4. FE operator training was inadequate for maintaining reliable operation.[d]

Reference: NERC Operating Policy 8:

SYSTEM OPERATOR Training. Each OPERATING AUTHORITY shall provide its SYSTEM OPERATORS with a coordinated training program that is designed to promote reliable operation. This program shall include:

- *Training staff. Individuals competent in both knowledge of system operations and instructional capabilities.*
- *Verification of achievement. Verification that all trainees have successfully demonstrated attainment of all required training objectives, including documented assessment of their training progress.*
- *Review. Periodic review to ensure that training materials are technically accurate and complete and to ensure that the training program continues to meet its objectives.*

Violation Number 5. MISO did not notify other reliability coordinators of potential problems.[e]

Reference: NERC Operating Policy 9:

Notify RELIABILITY COORDINATORS of potential problems. The RELIABILITY COORDINATOR who foresees a transmission problem within his RELIABILITY AREA shall issue an alert to all CONTROL AREAS and Transmission Providers in his RELIABILITY AREA, and all RELIABILITY COORDINATORS within the INTERCONNECTION via the RCIS without delay.

(continued on following page)

[a]Investigation team modeling showed that following the loss of the Chamberlin-Harding 345-kV line the system was beyond its OPERATING SECURITY LIMIT; i.e., the loss of the next most severe contingency would have resulted in other lines exceeding their emergency limits. Blackout causes 1A, 1B, 1E.

[b]DOE on-site interviews; comparative review of FE and MISO phone transcripts of 14 August; no calls found of FE declaring an emergency to MISO in either set of transcripts. Blackout causes 1A, 1B, 1D, 1E.

[c]DOE on-site interviews; Mr. Morgan, September 8 and 9 transcripts.

[d]Site visit by interviewers from Operations Team.

[e]MISO site visit and DOE interviews; Oct 1-3 Newark meetings, ns100303.pdf; Harzey-Cauley conversation, pages 111-119; blackout cause 3D.

Initial Findings: Violations of NERC Reliability Standards (Continued)

Violation Number 6. MISO did not have adequate monitoring capability.[f]

Reference: NERC Operating Policy 9, Appendix 9D:

> *Adequate facilities. Must have the facilities to perform their responsibilities, including:*
>
> - *Detailed monitoring capability of the RELIABILITY AREA and sufficient monitoring capability of the surrounding RELIABILITY AREAS to ensure potential security violations are identified.*

Continuous monitoring of Reliability Area. Must ensure that its RELIABILITY AREA of responsibility is continuously and adequately monitored. This includes the provisions for backup facilities.

[f]DOE interviews and Operations Team site visit. Oct 1-3 Newark meetings, ns100303.pdf; Harzey-Cauley conversation, pages 111-119; blackout causes 3A, 3B, 3C.

Energy Management System (EMS) and Decision Support Tools

Operators look at potential problems that could arise on their systems by using contingency analyses, driven from state estimation, that are fed by data collected by the SCADA system.

SCADA: System operators use **S**ystem **C**ontrol **a**nd **D**ata **A**cquisition systems to acquire power system data and control power system equipment. SCADA systems have three types of elements: field remote terminal units (RTUs), communication to and between the RTUs, and one or more Master Stations.

Field RTUs, installed at generation plants and substations, are combination data gathering and device control units. They gather and provide information of interest to system operators, such as the status of a breaker (switch), the voltage on a line or the amount of power being produced by a generator, and execute control operations such as opening or closing a breaker. Telecommunications facilities, such as telephone lines or microwave radio channels, are provided for the field RTUs so they can communicate with one or more SCADA Master Stations or, less commonly, with each other.

Master stations are the pieces of the SCADA system that initiate a cycle of data gathering from the field RTUs over the communications facilities, with the time cycles ranging from every few seconds to as long as several minutes. In many power systems, Master Stations are fully integrated into the control room, serving as the direct interface to the Energy Management System (EMS), receiving incoming data from the field RTUs and relaying control operations commands to the field devices for execution.

State Estimation: Transmission system operators have visibility (condition information) over their own transmission facilities. Most control facilities do not receive direct line voltage and current data on every facility for which they need visibility. Instead, system state estimators use the real-time data measurements available on a subset of those facilities in a complex mathematical model of the power system that reflects the configuration of the network (which facilities are in service and which are not) and real-time system condition data to estimate voltage at each bus, and to estimate real and reactive power flow quantities on each line or through each transformer. Reliability coordinators and control areas that have them commonly run a state estimator on regular intervals or only as the need arises (i.e., upon demand). Not all control areas use state estimators.

Contingency Analysis: Given the state estimator's representation of current system conditions, a system operator or planner uses contingency analysis to analyze the impact of specific outages (lines, generators, or other equipment) or higher load, flow, or generation levels on the security of the system. The contingency analysis should identify problems such as line overloads or voltage violations that will occur if a new event (contingency) happens on the system. Some transmission operators and control areas have and use state estimators to produce base cases from which to analyze next contingencies ("N-1," meaning normal system minus 1 element) from the current conditions. This tool is typically used to assess the reliability of system operation. Many control areas do not use real time contingency analysis tools, but others run them on demand following potentially significant system events.

Bloomington-Denois Creek 230-kV line—although it was out of service, its status was not updated in MISO's state estimator. Line status information within MISO's reliability coordination area is transmitted to MISO by the ECAR data network or direct links and intended to be automatically linked to the SE. This requires coordinated data naming as well as instructions that link the data to the tools. For this line, the automatic linkage of line status to the state estimator had not yet been established (this is an ongoing project at MISO). The line status was corrected and MISO's analyst obtained a good SE solution at 13:00 EDT and an RTCA solution at 13:07 EDT, but to troubleshoot this problem he had turned off the automatic trigger that runs the state estimator every five minutes. After fixing the problem he forgot to re-enable it, so although he had successfully run the SE and RTCA manually to reach a set of correct system analyses, the tools were not returned to normal automatic operation. Thinking the system had been successfully restored, the analyst went to lunch.

Cause 3: Inadequate RC Diagnostic Support

The fact that the state estimator was not running automatically on its regular 5-minute schedule was discovered about 14:40 EDT. The automatic trigger was re-enabled but again the state estimator failed to solve successfully. This time investigation identified the Stuart-Atlanta 345-kV line outage (14:02 EDT) to be the likely cause.[7] This line is jointly owned by Dayton Power and Light and AEP and is monitored by Dayton Power and Light and is under PJM's reliability umbrella rather than MISO's. Even though it affects electrical flows within MISO, its status had not been automatically linked to MISO's SE.

The discrepancy between actual measured system flows (with Stuart-Atlanta off-line) and the MISO model (which assumed Stuart-Atlanta on-line) prevented the state estimator from solving correctly. At 15:09 EDT, when informed by the system engineer that the Stuart-Atlanta line appeared to be the problem, the MISO operator said (mistakenly) that this line was in service. The system engineer then tried unsuccessfully to reach a solution with the Stuart-Atlanta line modeled as in service until approximately 15:29 EDT, when the MISO operator called PJM to verify the correct status. After they determined that Stuart-Atlanta had tripped, they updated the state estimator and it solved successfully. The RTCA was then run manually and solved successfully at 15:41 EDT. MISO's state estimator and contingency analysis were back under full automatic operation and solving effectively by 16:04 EDT, about two minutes before the initiation of the cascade.

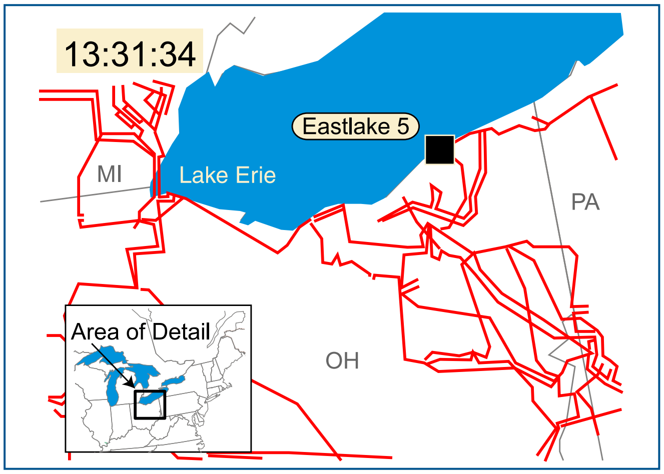
In summary, the MISO state estimator and real time contingency analysis tools were effectively out of service between 12:15 EDT and 16:04 EDT. This prevented MISO from promptly performing precontingency "early warning" assessments of power system reliability over the afternoon of August 14.

1B) Eastlake Unit 5 Tripped: 13:31 EDT

Eastlake Unit 5 (rated at 597 MW) is in northern Ohio along the southern shore of Lake Erie, connected to FE's 345-kV transmission system (Figure 4.3). The Cleveland and Akron loads are generally supported by generation from a combination of the Eastlake and Davis-Besse units, along with significant imports, particularly from 9,100 MW of generation located along the Ohio and Pennsylvania border. The unavailability of Eastlake 4 and Davis-Besse meant that FE had to import more energy into the Cleveland area (either from its own plants or from or through neighboring utilities) to support its load.

When Eastlake 5 dropped off-line, flows caused by replacement power transfers and the associated reactive power to support the imports to the local area contributed to the additional line loadings in the region. At 15:00 EDT on August 14, FE's load was approximately 12,080 MW. They were importing about 2,575 MW, 21% of their total. With this high level of imports, FE's system reactive power needs rose further. Investigation team modeling indicates that at about 15:00 EDT, FE's

Figure 4.3. Eastlake Unit 5



system was consuming so much reactive power that it was a net importer, bringing in about 132 MVAr.

The investigation team's system simulations indicate that the loss of Eastlake 5 was a critical step in the sequence of events. Contingency analysis simulation of the conditions following the loss of the Harding-Chamberlin 345-kV circuit at 15:05 EDT showed that the system would be unable to sustain some contingencies without line overloads above emergency ratings. However, when Eastlake 5 was modeled as in service and fully available in those simulations, all overloads above emergency limits were eliminated even with the loss of Harding-Chamberlin.

Cause 1:
Inadequate Situational Awareness

FE did not perform a contingency analysis after the loss of Eastlake 5 at 13:31 EDT to determine whether the loss of further lines or plants would put their system at risk. FE also did not perform a contingency analysis after the loss of Harding-Chamberlin at 15:05 EDT (in part because they did not know that it had tripped out of service), nor does the utility routinely conduct such studies.[8] Thus FE did not discover that their system was no longer in an N-1 secure state at 15:05 EDT, and that operator action was needed to remedy the situation.

1C) Stuart-Atlanta 345-kV Line Tripped: 14:02 EDT

Cause 3:
Inadequate RC Diagnostic Support

The Stuart-Atlanta 345-kV transmission line is in the control area of Dayton Power and Light.[9] At 14:02 EDT the line tripped due to contact with a tree, causing a short circuit to ground, and locked out. Investigation team modeling reveals that the loss of DPL's Stuart-Atlanta line had no significant electrical effect on power flows and voltages in the FE area. The team examined the security of FE's system, testing power flows and voltage levels with the combination of plant and line outages that evolved on the afternoon of August 14. This analysis shows that the availability or unavailability of the Stuart-Atlanta 345-kV line did not change the capability or performance of FE's system or affect any line loadings within the FE system, either immediately after its trip or later that afternoon. Again, the only reason why Stuart-Atlanta matters to the blackout is because it contributed to the failure of MISO's state estimator to operate effectively, so MISO could not fully identify FE's precarious system conditions until 16:04 EDT.

Phase 2: FE's Computer Failures: 14:14 EDT to 15:59 EDT

Overview of This Phase

Starting around 14:14 EDT, FE's control room operators lost the alarm function that provided audible and visual indications when a significant piece of equipment changed from an acceptable to problematic condition. Shortly thereafter, the EMS system lost a number of its remote control consoles. Next it lost the primary server computer that was hosting the alarm function, and then the backup server such that all functions that were being supported on these servers were stopped at 14:54 EDT. However, for over an hour no one in FE's control room grasped that their computer systems were not operating properly, even though FE's Information Technology support staff knew of the problems and were working to solve them, and the absence of alarms and other symptoms offered many clues to the operators of the EMS system's impaired state. Thus, without a functioning EMS or the knowledge that it had failed, FE's system operators remained unaware that their electrical system condition was beginning to degrade. Unknowingly, they used the outdated system condition information they did have to discount information from others about growing system problems.

Key Events in This Phase

2A) 14:14 EDT: FE alarm and logging software failed. Neither FE's control room operators nor FE's IT EMS support personnel were aware of the alarm failure.

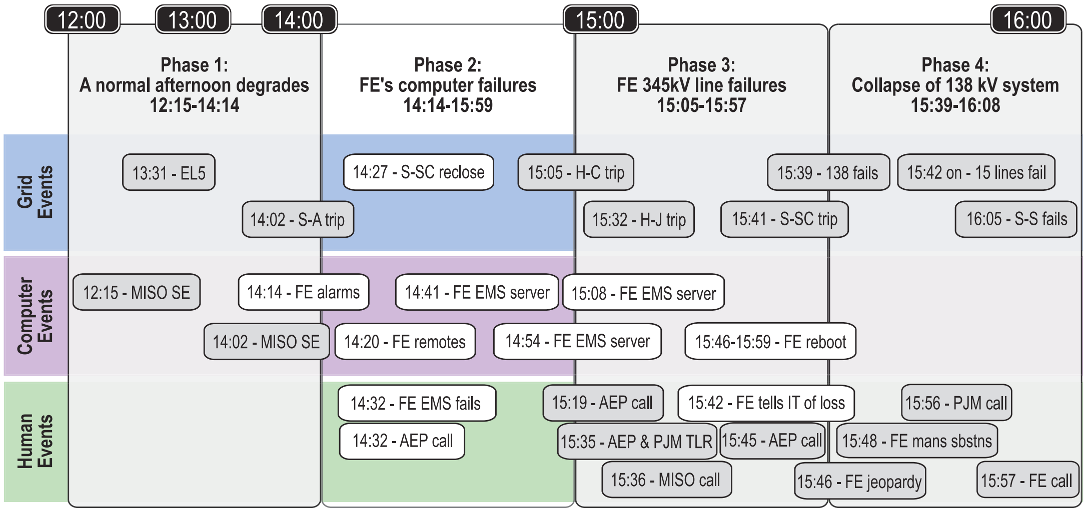
2B) 14:20 EDT: Several FE remote location consoles failed. FE Information Technology (IT) engineer was computer auto-paged.

2C) 14:27:16 EDT: Star-South Canton 345-kV transmission line tripped and successfully reclosed.

2D) 14:32 EDT: AEP called FE control room about AEP indication of Star-South Canton 345-kV line trip and reclosure. FE had no alarm or log of this line trip.

2E) 14:41 EDT: The primary FE control system server hosting the alarm function failed. Its applications and functions were passed over to a backup computer. FE's IT engineer was auto-paged.

Figure 4.4. Timeline Phase 2



2F) 14:54 EDT: The FE back-up computer failed and all functions that were running on it stopped. FE's IT engineer was auto-paged.

Failure of FE's Alarm System

Cause 1: Inadequate Situational Awareness

FE's computer SCADA alarm and logging software failed sometime shortly after 14:14 EDT (the last time that a valid alarm came in). After that time, the FE control room consoles did not receive any further alarms nor were there any alarms being printed or posted on the EMS's alarm logging facilities. Power system operators rely heavily on audible and on-screen alarms, plus alarm logs, to reveal any significant changes in their system's conditions. After 14:14 EDT on August 14, FE's operators were working under a significant handicap without these tools. However, they were in further jeopardy because they did not know that they were operating without alarms, so that they did not realize that system conditions were changing.

Alarms are a critical function of an EMS, and EMS-generated alarms are the fundamental means by which system operators identify events on the power system that need their attention. Without alarms, events indicating one or more significant system changes can occur but remain undetected by the operator. If an EMS's alarms are absent, but operators are aware of the situation and the remainder of the EMS's functions are intact, the operators can potentially continue to use the EMS to monitor and exercise control of their power system. In such circumstances, the operators would have to do so via repetitive, continuous manual scanning of numerous data and status points located within the multitude of individual displays available within their EMS. Further, it would be difficult for the operator to identify quickly the most relevant of the many screens available.

Although the alarm processing function of FE's EMS failed, the remainder of that system generally continued to collect valid real-time status information and measurements about FE's power system, and continued to have supervisory control over the FE system. The EMS also continued to send its normal and expected collection of information on to other monitoring points and authorities, including MISO and AEP. Thus these entities continued to receive accurate information about the status and condition of FE's power system even past the point when FE's EMS alarms failed. FE's operators were unaware that in this situation they needed to manually and more closely monitor and interpret the SCADA information they were receiving. Continuing on in the belief that their system was satisfactory and lacking any alarms from their EMS to the contrary, FE control room operators were subsequently surprised when they began receiving telephone calls from other locations and information sources—MISO, AEP, PJM, and FE field operations staff—who offered information on the status of FE's transmission facilities that conflicted with FE's system operators' understanding of the situation.

Analysis of the alarm problem performed by FE suggests that the alarm process essentially "stalled" while processing an alarm event, such that the process began to run in a manner that failed to complete the processing of that alarm or produce any other valid output (alarms). In the

meantime, new inputs—system condition data that needed to be reviewed for possible alarms—built up in and then overflowed the process' input buffers.[10]

Loss of Remote EMS Terminals. Between 14:20 EDT and 14:25 EDT, some of FE's remote control terminals in substations ceased operation. FE has advised the investigation team that it believes this occurred because the data feeding into those terminals started "queuing" and overloading the terminals' buffers. FE's system operators did not learn about this failure until 14:36 EDT, when a technician at one of the sites noticed the terminal was not working after he came in on the 15:00 shift, and called the main control room to report the problem. As remote terminals failed, each triggered an automatic page to FE's Information Technology (IT) staff.[11] The investigation team has not determined why some terminals failed whereas others did not. Transcripts indicate that data links to the remote sites were down as well.[12]

EMS Server Failures. FE's EMS system includes several server nodes that perform the higher functions of the EMS. Although any one of them can host all of the functions, FE's normal system configuration is to have a number of host subsets of the applications, with one server remaining in a "hot-standby" mode as a backup to the others should any fail. At 14:41 EDT, the primary server hosting the EMS alarm processing application failed, due either to the stalling of the alarm application, "queuing" to the remote terminals, or some combination of the two. Following preprogrammed instructions, the alarm system

Alarms

System operators must keep a close and constant watch on the multitude of things occurring simultaneously on their power system. These include the system's load, the generation and supply resources to meet that load, available reserves, and measurements of critical power system states, such as the voltage levels on the lines. Because it is not humanly possible to watch and understand all these events and conditions simultaneously, Energy Management Systems use alarms to bring relevant information to operators' attention. The alarms draw on the information collected by the SCADA real-time monitoring system.

Alarms are designed to quickly and appropriately attract the power system operator's attention to events or developments of interest on the system. They do so using combinations of audible and visual signals, such as sounds at operators' control desks and symbol or color changes or animations on system monitors or displays. EMS alarms for power systems are similar to the indicator lights or warning bell tones that a modern automobile uses to signal its driver, like the "door open" bell, an image of a headlight high beam, a "parking brake on" indicator, and the visual and audible alert when a gas tank is almost empty.

Power systems, like cars, use "status" alarms and "limit" alarms. A status alarm indicates the state of a monitored device. In power systems these are commonly used to indicate whether such items as switches or breakers are "open" or "closed" (off or on) when they should be otherwise, or whether they have changed condition since the last scan. These alarms should provide clear indication and notification to system operators of whether a given device is doing what they think it is, or what they want it to do—for instance, whether a given power line is connected to the system and moving power at a particular moment.

EMS limit alarms are designed to provide an indication to system operators when something important that is measured on a power system device—such as the voltage on a line or the amount of power flowing across it—is below or above pre-specified limits for using that device safely and efficiently. When a limit alarm activates, it provides an important early warning to the power system operator that elements of the system may need some adjustment to prevent damage to the system or to customer loads—rather like the "low fuel" or "high engine temperature" warnings in a car.

When FE's alarm system failed on August 14, its operators were running a complex power system without adequate indicators of when key elements of that system were reaching and passing the limits of safe operation—and without awareness that they were running the system without these alarms and should no longer trust the fact that they were not getting alarms as indicating that system conditions were still safe and not changing.

application and all other EMS software running on the first server automatically transferred ("failed-over") onto the back-up server. However, because the alarm application moved intact onto the backup while still stalled and ineffective, the backup server failed 13 minutes later, at 14:54 EDT. Accordingly, all of the EMS applications on these two servers stopped running.

The concurrent loss of both EMS servers apparently caused several new problems for FE's EMS and the operators who used it. Tests run during FE's after-the-fact analysis of the alarm failure event indicate that a concurrent absence of these servers can significantly slow down the rate at which the EMS system puts new—or refreshes existing—displays on operators' computer consoles. Thus at times on August 14th, operators' screen refresh rates—the rate at which new information and displays are painted onto the computer screen, normally 1 to 3 seconds—slowed to as long as 59 seconds per screen. Since FE operators have numerous information screen options, and one or more screens are commonly "nested" as sub-screens to one or more top level screens, operators' ability to view, understand and operate their system through the EMS would have slowed to a frustrating crawl.[13] This situation may have occurred between 14:54 EDT and 15:08 EDT when both servers failed, and again between 15:46 EDT and 15:59 EDT while FE's IT personnel attempted to reboot both servers to remedy the alarm problem.

Loss of the first server caused an auto-page to be issued to alert FE's EMS IT support personnel to the problem. When the back-up server failed, it too sent an auto-page to FE's IT staff. At 15:08 EDT, IT staffers completed a "warm reboot" (restart) of the primary server. Startup diagnostics monitored during that reboot verified that the computer and all expected processes were running; accordingly, FE's IT staff believed that they had successfully restarted the node and all the processes it was hosting. However, although the server and its applications were again running, the alarm system remained frozen and non-functional, even on the restarted computer. The IT staff did not confirm that the alarm system was again working properly with the control room operators.

Another casualty of the loss of both servers was the Automatic Generation Control (AGC) function hosted on those computers. Loss of AGC meant that FE's operators could not run affiliated power plants on pre-set programs to respond automatically to meet FE's system load and interchange obligations. Although the AGC did not work from 14:54 EDT to 15:08 EDT and 15:46 EDT to 15:59 EDT (periods when both servers were down), this loss of function does not appear to have had any effect on the blackout.

The concurrent loss of the EMS servers also caused the failure of FE's strip chart function. There are many strip charts in the FE Reliability Operator control room driven by the EMS computers, showing a variety of system conditions, including raw ACE (Area Control Error), FE System Load, and Sammis-South Canton and South Canton-Star loading. These charts are visible in the reliability operator control room. The chart printers continued to scroll but because the underlying computer system was locked up the chart pens showed only the last valid measurement recorded, without any variation from that measurement as time progressed; i.e. the charts "flat-lined." There is no indication that any operators noticed or reported the failed operation of the charts.[14] The few charts fed by direct analog telemetry, rather than the EMS system, showed primarily frequency data, and remained available throughout the afternoon of August 14. These yield little useful system information for operational purposes.

FE's Area Control Error (ACE), the primary control signal used to adjust generators and imports to match load obligations, did not function between 14:54 EDT and 15:08 EDT and later between 15:46 EDT and 15:59 EDT, when the two servers were down. This meant that generators were not controlled during these periods to meet FE's load and interchange obligations (except from 15:00 EDT to 15:09 EDT when control was switched to a backup controller). There were no apparent negative impacts due to this failure. It has not been established how loss of the primary generation control signal was identified or if any discussions occurred with respect to the computer system's operational status.[15]

EMS System History. The EMS in service at FE's Ohio control center is a GE Harris (now GE Network Systems) XA21 system. It was initially brought into service in 1995. Other than the application of minor software fixes or patches typically encountered in the ongoing maintenance and support of such a system, the last major updates or revisions to this EMS were implemented in 1998. On August 14 the system was not running the most current release of the XA21 software. FE had

decided well before August 14 to replace it with one from another vendor.

FE personnel told the investigation team that the alarm processing application had failed on occasions prior to August 14, leading to loss of the alarming of system conditions and events for FE's operators.[16] However, FE said that the mode and behavior of this particular failure event were both first time occurrences and ones which, at the time, FE's IT personnel neither recognized nor knew how to correct. FE staff told investigators that it was only during a post-outage support call with GE late on 14 August that FE and GE determined that the only available course of action to correct the alarm problem was a "cold reboot"[17] of FE's overall XA21 system. In interviews immediately after the blackout, FE IT personnel indicated that they discussed a cold reboot of the XA21 system with control room operators after they were told of the alarm problem at 15:42 EDT, but decided not to take such action because operators considered power system conditions precarious, were concerned about the length of time that the reboot might take to complete, and understood that a cold boot would leave them with even less EMS support until it was completed.[18]

Clues to the EMS Problems. There is an entry in FE's western desk operator's log at 14:14 EDT referring to the loss of alarms, but it is not clear whether that entry was made at that time or subsequently, referring back to the last known alarm. There is no indication that the operator mentioned the problem to other control room staff and supervisors or to FE's IT staff.

The first clear hint to FE control room staff of any computer problems occurred at 14:19 EDT when a caller and an FE control room operator discussed the fact that three sub-transmission center dial-ups had failed.[19] At 14:25 EDT, a control room operator talked with a caller about the failure of these three remote terminals.[20] The next

Who Saw What?

What data and tools did others have to monitor the conditions on the FE system?

Midwest ISO (MISO), reliability coordinator for FE

Alarms: MISO received indications of breaker trips in FE that registered in their alarms. These alarms were missed. These alarms require a look-up to link the flagged breaker with the associated line or equipment and unless this line was specifically monitored, require another look-up to link the line to the monitored flowgate. MISO operators did not have the capability to click on the on-screen alarm indicator to display the underlying information.

Real Time Contingency Analysis (RTCA): The contingency analysis showed several hundred violations around 15:00 EDT. This included some FE violations, which MISO (FE's reliability coordinator) operators discussed with PJM (AEP's Reliability Coordinator).[a] Simulations developed for this investigation show that violations for a contingency would have occurred after the Harding-Chamberlin trip at 15:05 EDT. There is no indication that MISO addressed this issue. It is not known whether MISO identified the developing Sammis-Star problem.

Flowgate Monitoring Tool: While an inaccuracy has been identified with regard to this tool it still functioned with reasonable accuracy and prompted MISO to call FE to discuss the Hanna-Juniper line problem. It would not have identified problems south of Star since that was not part of the flowgate and thus not modeled in MISO's flowgate monitor.

AEP

Contingency Analysis: According to interviews,[b] AEP had contingency analysis that covered lines into Star. The AEP operator identified a problem for Star-South Canton overloads for a Sammis-Star line loss about 15:33 EDT and asked PJM to develop TLRs for this.

Alarms: Since a number of lines cross between AEP's and FE's systems, they had the ability at their respective end of each line to identify contingencies that would affect both. AEP initially noticed FE line problems with the first and subsequent trippings of the Star-South Canton 345-kV line, and called FE three times between 14:35 EDT and 15:45 EDT to determine whether FE knew the cause of the outage.[c]

[a] "MISO Site Visit," Benbow interview.
[b] "AEP Site Visit," Ulrich interview.
[c] Example at 14:35, Channel 4; 15:19, Channel 4; 15:45, Channel 14 (FE transcripts).

hint came at 14:32 EDT, when FE scheduling staff spoke about having made schedule changes to update the EMS pages, but that the totals did not update.[21]

Although FE's IT staff would have been aware that concurrent loss of its servers would mean the loss of alarm processing on the EMS, the investigation team has found no indication that the IT staff informed the control room staff either when they began work on the servers at 14:54 EDT, or when they completed the primary server restart at 15:08 EDT. At 15:42 EDT, the IT staff were first told of the alarm problem by a control room operator; FE has stated to investigators that their IT staff had been unaware before then that the alarm processing sub-system of the EMS was not working.

Cause 1: Inadequate Situational Awareness

Without the EMS systems, the only remaining ways to monitor system conditions would have been through telephone calls and direct analog telemetry. FE control room personnel did not realize that alarm processing on their EMS was not working and, subsequently, did not monitor other available telemetry.

Cause 1: Inadequate Situational Awareness

During the afternoon of August 14, FE operators talked to their field personnel, MISO, PJM (concerning an adjoining system in PJM's reliability coordination region), adjoining systems (such as AEP), and customers. The FE operators received pertinent information from all these sources, but did not grasp some key information about the system from the clues offered. This pertinent information included calls such as that from FE's eastern control center where they were asking about possible line trips, FE Perry nuclear plant calls regarding what looked like near-line trips, AEP calling about their end of the Star-South Canton line tripping, and MISO and PJM calling about possible line overloads.

Without a functioning alarm system, the FE control area operators failed to detect the tripping of electrical facilities essential to maintain the security of their control area. Unaware of the loss of alarms and a limited EMS, they made no alternate arrangements to monitor the system. When AEP identified a circuit trip and reclosure on a 345-kV line, the FE operator dismissed the information as either not accurate or not relevant to his system, without following up on the discrepancy between the AEP event and the information from his own tools. There was no subsequent verification of conditions with their MISO reliability coordinator. Only after AEP notified FE that a 345-kV circuit had tripped and locked out did the FE control area operator compare this information to the breaker statuses for their station. FE failed to inform immediately its reliability coordinator and adjacent control areas when they became aware that system conditions had changed due to unscheduled equipment outages that might affect other control areas.

Phase 3: Three FE 345-kV Transmission Line Failures and Many Phone Calls: 15:05 EDT to 15:57 EDT

Overview of This Phase

From 15:05:41 EDT to 15:41:35 EDT, three 345-kV lines failed with power flows at or below each transmission line's emergency rating. Each was the result of a contact between a line and a tree that had grown so tall that, over a period of years, it encroached into the required clearance height for the line. As each line failed, its outage increased the loading on the remaining lines (Figure 4.5). As each of the transmission lines failed, and power flows shifted to other transmission paths, voltages on the rest of FE's system degraded further (Figure 4.6).

Key Phase 3 Events

3A) 15:05:41 EDT: Harding-Chamberlin 345-kV line tripped.

3B) 15:31-33 EDT: MISO called PJM to determine if PJM had seen the Stuart-Atlanta 345-kV line outage. PJM confirmed Stuart-Atlanta was out.

Figure 4.5. FirstEnergy 345-kV Line Flows

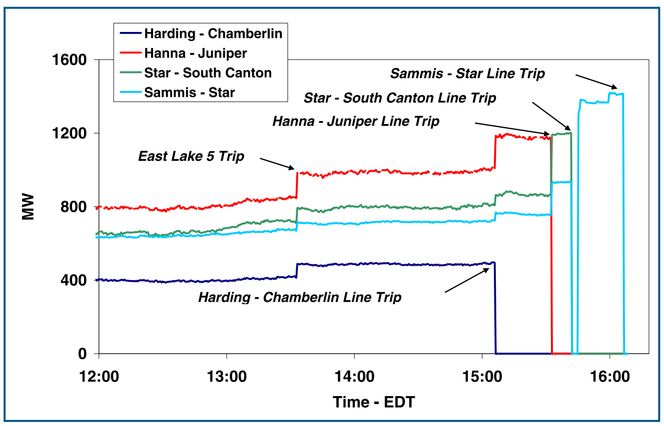
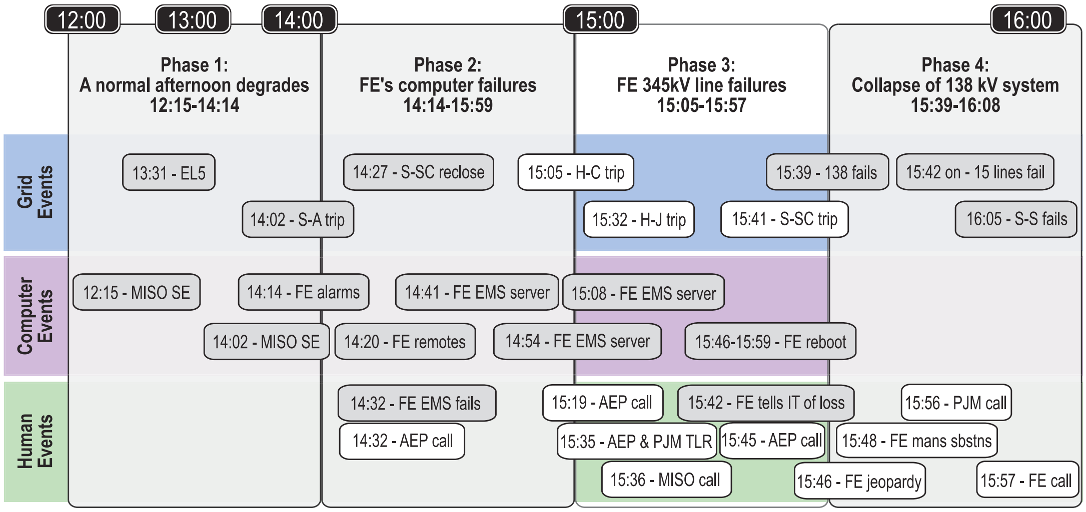


Figure 4.7. Timeline Phase 3



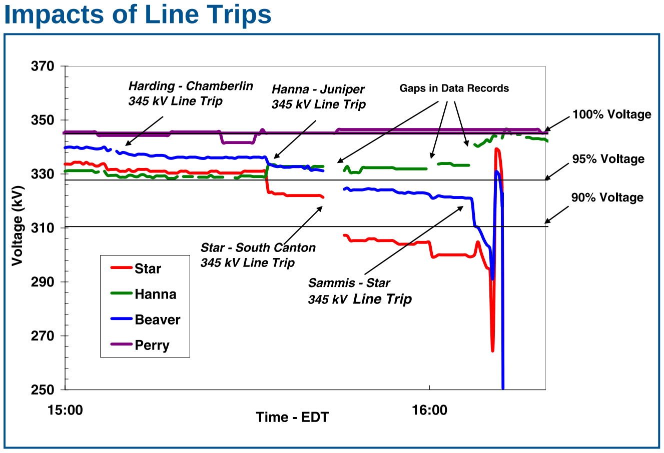
3C) 15:32:03 EDT: Hanna-Juniper 345-kV line tripped.

3D) 15:35 EDT: AEP asked PJM to begin work on a 350-MW TLR to relieve overloading on the Star-South Canton line, not knowing the Hanna-Juniper 345-kV line had already tripped at 15:32 EDT.

3E) 15:36 EDT: MISO called FE regarding post-contingency overload on Star-Juniper 345-kV line for the contingency loss of the Hanna-Juniper 345-kV line, unaware at the start of the call that Hanna-Juniper had already tripped.

3F) 15:41:33-41 EDT: Star-South Canton 345-kV tripped, reclosed, tripped again at 15:41 EDT and remained out of service, all while AEP and PJM were discussing TLR relief options (event 3D).

Figure 4.6. Voltages on FirstEnergy's 345-kV Lines: Impacts of Line Trips



Transmission lines are designed with the expectation that they will sag lower when they are hotter. The transmission line gets hotter with heavier line loading and under higher ambient temperatures, so towers and conductors are designed to be tall enough and conductors pulled tightly enough to accommodate expected sagging.

A short-circuit occurred on the Harding-Chamberlin 345-kV line due to a contact between the line conductor and a tree. This line failed with power flow at only 43.5% of its normal and emergency line rating. Incremental line current and temperature increases, escalated by the loss of Harding-Chamberlin, caused enough sag on the Hanna-Juniper line that it contacted a tree and faulted with power flow at 87.5% of its normal and emergency line rating. Star-South Canton contacted a tree three times between 14:27:15 EDT and 15:41:33 EDT, opening and reclosing each time before finally locking out while loaded at 93.2% of its emergency rating at 15:42:35 EDT.

Cause 2: Inadequate Tree Trimming

Overgrown trees, as opposed to excessive conductor sag, caused each of these faults. While sag may have contributed to these events, these incidents occurred because the trees grew too tall and encroached into the space below the line which is intended to be clear of any objects, not because the lines sagged into short trees. Because the trees were so tall (as discussed below), each of these lines faulted under system conditions well within specified operating parameters. The investigation team found field evidence of tree contact at all three locations, although Hanna-Juniper is the only one with a confirmed sighting for the August 14

Line Ratings

A conductor's normal rating reflects how heavily the line can be loaded under routine operation and keep its internal temperature below 90°C. A conductor's emergency rating is often set to allow higher-than-normal power flows, but to limit its internal temperature to a maximum of 100°C for no longer than a short, specified period, so that it does not sag too low. For three of the four 345-kV lines that failed, FE set the normal and emergency ratings at the same level.

tree/line contact. For the other locations, the team found various types of evidence, outlined below, that confirm that contact with trees caused the short circuits to ground that caused each line to trip out on August 14.

To be sure that the evidence of tree/line contacts and tree remains found at each site was linked to the events of August 14, the team looked at whether these lines had any prior history of outages in preceding months or years that might have resulted in the burn marks, debarking, and other vegetative evidence of line contacts. The record establishes that there were no prior sustained outages known to be caused by trees for these lines in 2001, 2002 and 2003.[22]

Like most transmission owners, FE patrols its lines regularly, flying over each transmission line twice a year to check on the condition of the rights-of-way. Notes from fly-overs in 2001 and 2002 indicate that the examiners saw a significant number of trees and brush that needed clearing or trimming along many FE transmission lines.

Utility Vegetation Management: When Trees and Lines Contact

Vegetation management is critical to any utility company that maintains overhead energized lines. It is important and relevant to the August 14 events because electric power outages occur when trees, or portions of trees, grow up or fall into overhead electric power lines. While not all outages can be prevented (due to storms, heavy winds, etc.), many outages can be mitigated or prevented by managing the vegetation *before* it becomes a problem. When a tree contacts a power line it causes a short circuit, which is read by the line's relays as a ground fault. Direct physical contact is not necessary for a short circuit to occur. An electric arc can occur between a part of a tree and a nearby high-voltage conductor if a sufficient distance separating them is not maintained. Arcing distances vary based on such factors such as voltage and ambient wind and temperature conditions. Arcs can cause fires as well as short circuits and line outages.

Most utilities have right-of-way and easement agreements allowing the utility to clear and maintain the vegetation as needed along its lines to provide safe and reliable electric power. Easements give the utility a great deal of control over the landscape, with extensive rights to do whatever work is required to maintain the lines with adequate clearance through the control of vegetation. The three principal means of managing vegetation along a transmission right-of-way are pruning the limbs adjacent to the line clearance zone, removing vegetation completely by mowing or cutting, and using herbicides to retard or kill further growth. It is common to see more tree and brush removal using mechanical and chemical tools and relatively less pruning along transmission rights-of-way.

FE's easement agreements establish extensive rights regarding what can be pruned or removed in these transmission rights-of-way, including: "the right to erect, inspect, operate, replace, relocate, repair, patrol and permanently maintain upon, over, under and along the above described right of way across said premises all necessary structures, wires, cables and other usual fixtures and appurtenances used for or in connection with the transmission and distribution of electric current, including telephone and telegraph, and the right to trim, cut, remove or control by any other means at any and all times such trees, limbs and underbrush within or adjacent to said right of way as may interfere with or endanger said structures, wires or appurtenances, or their operations."[a]

FE uses a 5-year cycle for transmission line vegetation maintenance, i.e. completes all required vegetation work within a five year period for all circuits. A 5-year cycle is consistent with industry standards, and it is common for transmission providers not to fully exercise their easement rights on transmission rights-of-way due to landowner opposition.

[a]Standard language in FE's right-of-way easement agreement.

3A) FE's Harding-Chamberlin 345-kV Line Tripped: 15:05 EDT

Cause 2: Inadequate Tree Trimming

At 15:05:41 EDT, FE's Harding-Chamberlin line (Figure 4.8) tripped and locked out while loaded at 43.5% of its normal and emergency rating. The investigation team has examined the relay data for this trip, identified the geographic location of the fault, and determined that the relay data match the classic "signature" pattern for a tree/line short circuit to ground fault. Going to the fault location determined from the relay data, the field team found the remains of trees and brush. At this location, conductor height measured 46 feet 7 inches, while the height of the felled tree measured 42 feet; however, portions of the tree had been removed from the site. This means that while it is difficult to determine the exact height of the line contact, the measured height is a minimum and the actual contact was likely 3 to 4 feet higher than estimated here. Burn marks were observed 35 feet 8 inches up the tree, and the crown of this tree was at least 6 feet taller than the observed burn marks. The tree showed evidence of fault current damage.[23]

When the Harding-Chamberlin line locked out, the loss of this 345-kV path caused the remaining three southern 345-kV lines into Cleveland to pick up more load, with Hanna-Juniper picking up the most. The Harding-Chamberlin outage also caused more power to flow through the underlying 138-kV system.

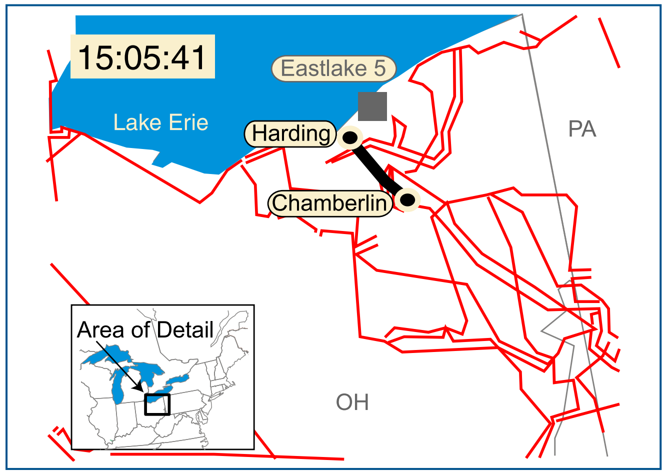
Cause 1: Inadequate Situational Awareness

MISO did not discover that Harding-Chamberlin had tripped until after the blackout, when MISO reviewed the breaker operation log that evening. FE indicates that it discovered the line was out while investigating system conditions in response MISO's call at 15:36 EDT, when MISO told FE that MISO's flowgate monitoring tool showed a Star-Juniper line overload following a contingency loss of Hanna-Juniper;[24] however, the investigation team has found no evidence within the control room logs or transcripts to show that FE knew of the Harding-Chamberlin line failure until after the blackout.

Cause 3: Inadequate RC Diagnostic Support

Harding-Chamberlin was not one of the flowgates that MISO monitored as a key transmission location, so the reliability coordinator was unaware when FE's first 345-kV line failed. Although MISO received SCADA input of the line's status change, this was presented to MISO operators as breaker status changes rather than a line failure. Because their EMS system topology processor had not yet been linked to recognize line failures, it did not connect the breaker information to the loss of a transmission line. Thus, MISO's operators did not recognize the Harding-Chamberlin trip as a significant contingency event and could not advise FE regarding the event or its consequences. Further, without its state estimator and associated contingency analyses, MISO was unable to identify potential overloads that would occur due to various line or equipment outages. Accordingly, when the Harding-Chamberlin 345-kV line tripped at 15:05 EDT, the state estimator did not produce results and could not predict an overload if the Hanna-Juniper 345-kV line were to fail.[25]

Figure 4.8. Harding-Chamberlin 345-kV Line



3C) FE's Hanna-Juniper 345-kV Line Tripped: 15:32 EDT

Cause 2: Inadequate Tree Trimming

At 15:32:03 EDT the Hanna-Juniper line (Figure 4.9) tripped and locked out. A tree-trimming crew was working nearby and observed the tree/line contact. The tree contact occurred on the South phase, which is lower than the center phase due to construction design. Although little evidence remained of the tree during the field team's visit in October, the team observed a tree stump 14 inches in diameter at its ground line and talked to an individual who witnessed the contact on August 14.[26] FE provided photographs that clearly indicate that the tree was of excessive height. Surrounding trees were 18 inches in diameter at ground line and 60 feet in height (not near lines). Other sites at this location had numerous (at least 20) trees in this right-of-way.

Figure 4.9. Hanna-Juniper 345-kV Line

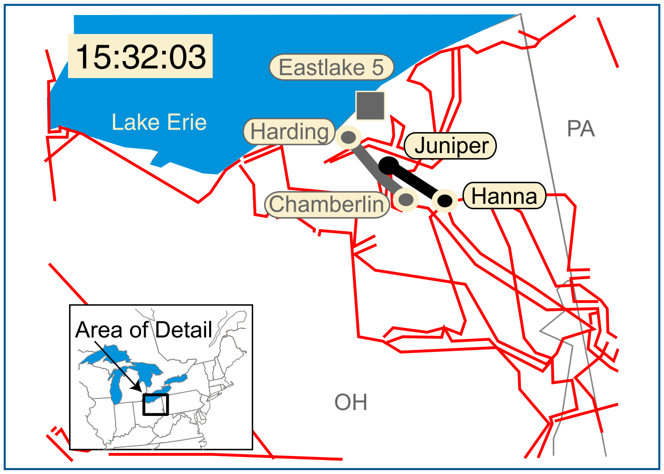
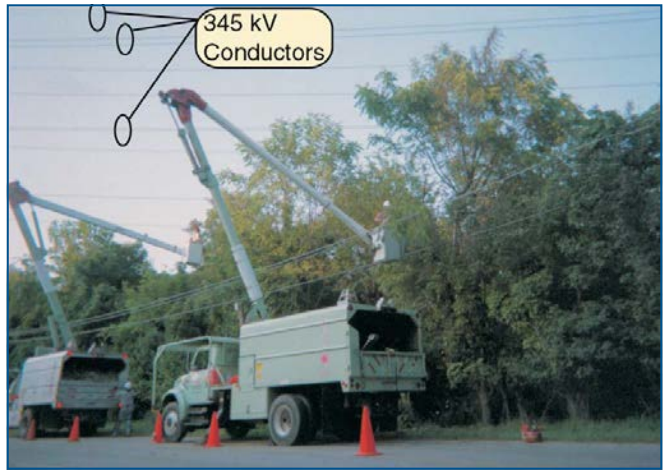


Figure 4.10. Cause of the Hanna-Juniper Line Loss



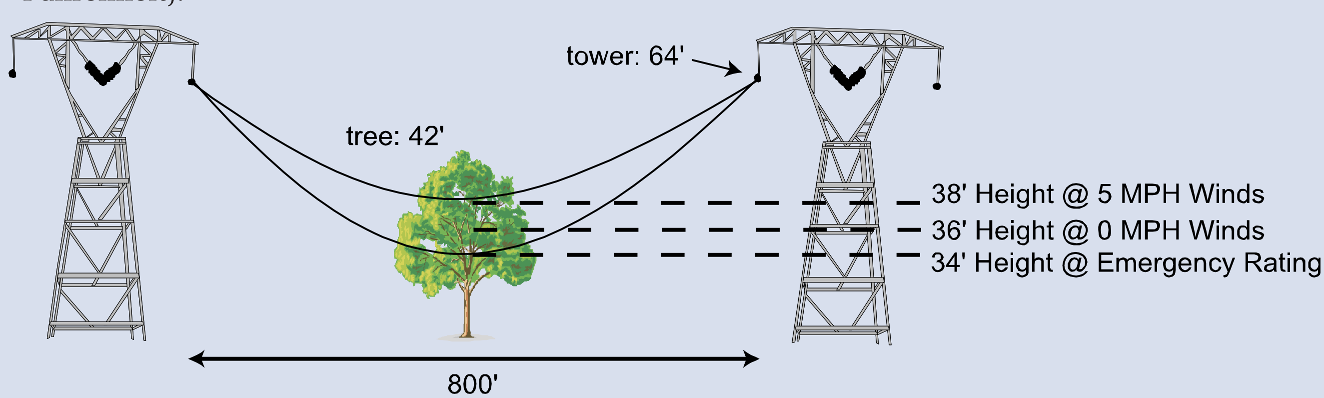
This August 14 photo shows the tree that caused the loss of the Hanna-Juniper line (tallest tree in photo). Other 345-kV conductors and shield wires can be seen in the background. Photo by Nelson Tree.

Why Did So Many Tree-to-Line Contacts Happen on August 14?

Tree-to-line contacts and resulting transmission outages are not unusual in the summer across much of North America. The phenomenon occurs because of a combination of events occurring particularly in late summer:

- Most tree growth occurs during the spring and summer months, so the later in the summer the taller the tree and the greater its potential to contact a nearby transmission line.
- As temperatures increase, customers use more air conditioning and load levels increase. Higher load levels increase flows on the transmission system, causing greater demands for both active power (MW) and reactive power (MVAr). Higher flow on a transmission line causes the line to heat up, and the hot line sags lower because the hot conductor metal expands. Most emergency line ratings are set to limit conductors' internal temperatures to no more than 100 degrees Celsius (212 degrees Fahrenheit).
- As temperatures increase, ambient air temperatures provide less cooling for loaded transmission lines.
- Wind flows cool transmission lines by increasing the airflow of moving air across the line. On August 14 wind speeds at the Ohio Akron-Fulton airport averaged 5 knots at around 14:00 EDT, but by 15:00 EDT wind speeds had fallen to 2 knots (the wind speed commonly assumed in conductor design) or lower. With lower winds, the lines sagged further and closer to any tree limbs near the lines.

This combination of events on August 14 across much of Ohio and Indiana caused transmission lines to heat and sag. If a tree had grown into a power line's designed clearance area, then a tree/line contact was more likely, though not inevitable. An outage on one line would increase power flows on related lines, causing them to be loaded higher, heat further, and sag lower.



Hanna-Juniper was loaded at 87.5% of its normal and emergency rating when it tripped. With this line open, almost 1,000 MVA had to find a new path to reach its load in Cleveland. Loading on the remaining two 345-kV lines increased, with Star-Juniper taking the bulk of the power. This caused Star-South Canton's loading to rise above its normal but within its emergency rating and pushed more power onto the 138-kV system. Flows west into Michigan decreased slightly and voltages declined somewhat in the Cleveland area.

3D) AEP and PJM Begin Arranging a TLR for Star-South Canton: 15:35 EDT

Cause 3: Inadequate RC Diagnostic Support

Because its alarm system was not working, FE was not aware of the Harding-Chamberlin or Hanna-Juniper line trips. However, once MISO manually updated the state estimator model for the Stuart-Atlanta 345-kV line outage, the software successfully completed a state estimation and contingency analysis at 15:41 EDT. But this left a 36 minute period, from 15:05 EDT to 15:41 EDT, during which MISO did not recognize the consequences of the Hanna-Juniper loss, and FE operators knew neither of the line's loss nor its consequences. PJM and AEP recognized the overload on Star-South Canton, but had not expected it because their earlier contingency analysis did not examine enough lines within the FE system to foresee this result of the Hanna-Juniper contingency on top of the Harding-Chamberlin outage.

Cause 3: Inadequate RC Diagnostic Support

After AEP recognized the Star-South Canton overload, at 15:35 EDT AEP asked PJM to begin developing a 350-MW TLR to mitigate it. The TLR was to relieve the actual overload above normal rating then occurring on Star-South Canton, and prevent an overload above emergency rating on that line if the Sammis-Star line were to fail. But when they began working on the TLR, neither AEP nor PJM realized that the Hanna-Juniper 345-kV line had

Handling Emergencies by Shedding Load and Arranging TLRs

Transmission loading problems. Problems such as contingent overloads or contingent breaches of stability limits are typically handled by arranging Transmission Loading Relief (TLR) measures, which in most cases take effect as a schedule change 30 to 60 minutes after they are issued. Apart from a TLR level 6, TLRs are intended as a tool to prevent the system from being operated in an unreliable state,[a] and are not applicable in real-time emergency situations because it takes too long to implement reductions. Actual overloads and violations of stability limits need to be handled immediately under TLR level 6 by redispatching generation, system reconfiguration or tripping load. The dispatchers at FE, MISO and other control areas or reliability coordinators have authority—and under NERC operating policies, responsibility—to take such action, but the occasion to do so is relatively rare.

Lesser TLRs reduce scheduled transactions—non-firm first, then pro-rata between firm transactions, including native load. When pre-contingent conditions are not solved with TLR levels 3 and 5, or conditions reach actual overloading or surpass stability limits, operators must use emergency generation redispatch and/or load-shedding under TLR level 6 to return to a secure state. After a secure state is reached, TLR level 3 and/or 5 can be initiated to relieve the emergency generation redispatch or load-shedding activation.

System operators and reliability coordinators, by NERC policy, have the responsibility and the authority to take actions up to and including emergency generation redispatch and shedding firm load to preserve system security. On August 14, because they either did not know or understand enough about system conditions at the time, system operators at FE, MISO, PJM, or AEP did not call for emergency actions.

Use of automatic procedures in voltage-related emergencies. There are few automatic safety nets in place in northern Ohio except for under-frequency load-shedding in some locations. In some utility systems in the U.S. Northeast, Ontario, and parts of the Western Interconnection, special protection systems or remedial action schemes, such as under-voltage load-shedding are used to shed load under defined severe contingency conditions similar to those that occurred in northern Ohio on August 14.

[a]"Northern MAPP/Northwestern Ontario Disturbance-June 25, 1998," NERC 1998 Disturbance Report, page 17.

already tripped at 15:32 EDT, further degrading system conditions. Since the great majority of TLRs are for cuts of 25 to 50 MW, a 350-MW TLR request was highly unusual and operators were attempting to confirm why so much relief was suddenly required before implementing the requested TLR. Less than ten minutes elapsed between the loss of Hanna-Juniper, the overload above the normal limits of Star-South Canton, and the Star-South Canton trip and lock-out.

Cause 3: Inadequate RC Diagnostic Support

The primary tool MISO uses for assessing reliability on key flowgates (specified groupings of transmission lines or equipment that sometimes have less transfer capability than desired) is the flowgate monitoring tool. After the Harding-Chamberlin 345-kV line outage at 15:05 EDT, the flowgate monitoring tool produced incorrect (obsolete) results, because the outage was not reflected in the model. As a result, the tool assumed that Harding-Chamberlin was still available and did not predict an overload for loss of the Hanna-Juniper 345-kV line. When Hanna-Juniper tripped at 15:32 EDT, the resulting overload was detected by MISO's SCADA and set off alarms to MISO's system operators, who then phoned FE about it.[27] Because both MISO's state estimator, which was still in a developmental state, and its flowgate monitoring tool were not working properly, MISO's ability to recognize FE's evolving contingency situation was impaired.

3F) Loss of the Star-South Canton 345-kV Line: 15:41 EDT

The Star-South Canton line (Figure 4.11) crosses the boundary between FE and AEP, and the line is jointly owned—each company owns the portion of the line within its respective territory and manages the right-of-way there. The Star-South Canton line tripped and reclosed three times on the afternoon of August 14, first at 14:27:15 EDT (reclosing at both ends), then at 15:38:48 EDT, and at 15:41:35 EDT it tripped and locked out at the Star substation. A short-circuit to ground occurred in each case. This line failed with power flow at 93.2% of its emergency rating.

Cause 2: Inadequate Tree Trimming

The investigation field team inspected the right of way in the location indicated by the relay digital fault recorders, in the FE portion of the line. They found debris from trees and vegetation that had been felled. At this location the conductor height was 44 feet 9 inches. The identifiable tree remains measured 30 feet in height, although the team could not verify the location of the stump, nor find all sections of the tree. A nearby cluster of trees showed significant fault damage, including charred limbs and de-barking from fault current. Further, topsoil in the area of the tree trunk was disturbed, discolored and broken up, a common indication of a higher magnitude fault or multiple faults. Analysis of another stump showed that a fourteen year-old tree had recently been removed from the middle of the right-of-way.[28]

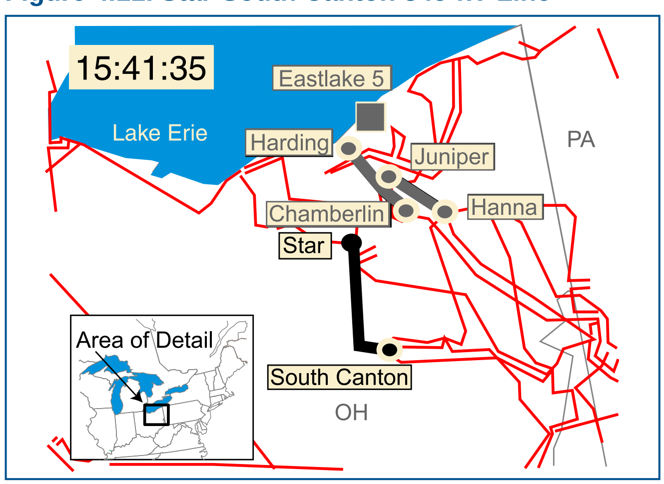
After the Star-South Canton line was lost, flows increased greatly on the 138-kV system toward Cleveland and area voltage levels began to degrade on the 138-kV and 69-kV system. At the same time, power flows increased on the Sammis-Star 345-kV line due to the 138-kV line trips—the only remaining paths into Cleveland from the south.

Cause 1: Inadequate Situational Awareness

FE's operators were not aware that the system was operating outside first contingency limits after the Harding-Chamberlin trip (for the possible loss of Hanna-Juniper), because they did not conduct a contingency analysis.[29] The investigation team has not determined whether the system status information used by FE's state estimator and contingency analysis model was being accurately updated.

System impacts of the 345-kV failures. The investigation modeling team examined the impact of the loss of the Harding-Chamberlin, Hanna-Juniper and Star-South Canton 345-kV lines. After conducting a variety of scenario analyses, they concluded that had either Hanna-Juniper or Harding-Chamberlin been restored and remained in-service, the Star-South Canton line might not have tripped and locked out at 15:42 EDT.

Figure 4.11. Star-South Canton 345-kV Line

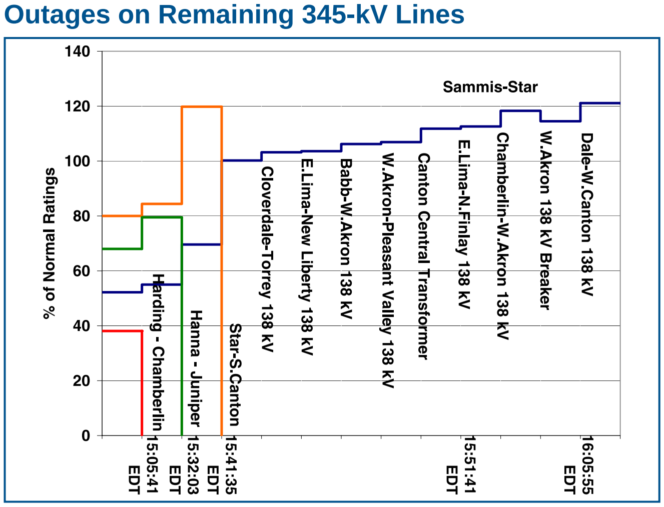


According to extensive investigation team modeling, there were no contingency limit violations as of 15:05 EDT prior to the loss of the Chamberlin-Harding 345-kV line. Figure 4.12 shows the line loadings estimated by investigation team modeling as the 345-kV lines in northeast Ohio began to trip. Showing line loadings on the 345-kV lines as a percent of normal rating, it tracks how the loading on each line increased as each subsequent 345-kV and 138-kV line tripped out of service between 15:05 EDT (Harding-Chamberlin, the first line above to stair-step down) and 16:06 EDT (Dale-West Canton). As the graph shows, none of the 345- or 138-kV lines exceeded their normal ratings until after the combined trips of Harding-Chamberlin and Hanna-Juniper. But immediately after the second line was lost, Star-South Canton's loading jumped from an estimated 82% of normal to 120% of normal (which was still below its emergency rating) and remained at the 120% level for 10 minutes before tripping out. To the right, the graph shows the effects of the 138-kV line failures (discussed in the next phase) upon the two remaining 345-kV lines—i.e., Sammis-Star's loading increased steadily above 100% with each succeeding 138-kV line lost.

Following the loss of the Harding-Chamberlin 345-kV line at 15:05 EDT, contingency limit violations existed for:

- The Star-Juniper 345-kV line, whose loadings would exceed emergency limits if the Hanna-Juniper 345-kV line were lost; and
- The Hanna-Juniper and Harding-Juniper 345-kV lines, whose loadings would exceed emergency limits if the Perry generation unit (1,255 MW) were lost.

Figure 4.12. Cumulative Effects of Sequential Outages on Remaining 345-kV Lines



Operationally, once FE's system entered an N-1 contingency violation state, any facility loss beyond that pushed them farther into violation and into a more unreliable state. After loss of the Harding-Chamberlin line, to avoid violating NERC criteria, FE needed to reduce loading on these three lines within 30 minutes such that no single contingency would violate an emergency limit; that is, to restore the system to a reliable operating mode.

Phone Calls into the FE Control Room

Cause 1: Inadequate Situational Awareness

Beginning no earlier than 14:14 EDT when their EMS alarms failed, and until at least 15:42 EDT when they began to recognize their situation, FE operators did not understand how much of their system was being lost, and did not realize the degree to which their perception of their system was in error versus true system conditions, despite receiving clues via phone calls from AEP, PJM and MISO, and customers. The FE operators were not aware of line outages that occurred after the trip of Eastlake 5 at 13:31 EDT until approximately 15:45 EDT, although they were beginning to get external input describing aspects of the system's weakening condition. Since FE's operators were not aware and did not recognize events as they were occurring, they took no actions to return the system to a reliable state.

A brief description follows of some of the calls FE operators received concerning system problems and their failure to recognize that the problem was on their system. For ease of presentation, this set of calls extends past the time of the 345-kV line trips into the time covered in the next phase, when the 138-kV system collapsed.

Following the first trip of the Star-South Canton 345-kV line at 14:27 EDT, AEP called FE at 14:32 EDT to discuss the trip and reclose of the line. AEP was aware of breaker operations at their end (South Canton) and asked about operations at FE's Star end. FE indicated they had seen nothing at their end of the line but AEP reiterated that the trip occurred at 14:27 EDT and that the South Canton breakers had reclosed successfully.[30] There was an internal FE conversation about the AEP call at 14:51 EDT, expressing concern that they had not seen any indication of an operation, but lacking evidence within their control room, the FE operators did not pursue the issue.

At 15:19 EDT, AEP called FE back to confirm that the Star-South Canton trip had occurred and that

AEP had a confirmed relay operation from the site. FE's operator restated that because they had received no trouble or alarms, they saw no problem. An AEP technician at the South Canton substation verified the trip. At 15:20 EDT, AEP decided to treat the South Canton digital fault recorder and relay target information as a "fluke," and checked the carrier relays to determine what the problem might be.[31]

At 15:35 EDT the FE control center received a call from the Mansfield 2 plant operator concerned about generator fault recorder triggers and excitation voltage spikes with an alarm for over-excitation, and a dispatcher called reporting a "bump" on their system. Soon after this call, FE's Reading, Pennsylvania control center called reporting that fault recorders in the Erie west and south areas had activated, wondering if something had happened in the Ashtabula-Perry area. The Perry nuclear plant operator called to report a "spike" on the unit's main transformer. When he went to look at the metering it was "still bouncing around pretty good. I've got it relay tripped up here … so I know something ain't right."[32]

Beginning at this time, the FE operators began to think that something was wrong, but did not recognize that it was on their system. "It's got to be in distribution, or something like that, or somebody else's problem … but I'm not showing anything."[33] Unlike many other transmission grid control rooms, FE's control center does not have a map board (which shows schematically all major lines and plants in the control area on the wall in front of the operators), which might have shown the location of significant line and facility outages within the control area.

At 15:36 EDT, MISO contacted FE regarding the post-contingency overload on Star-Juniper for the loss of the Hanna-Juniper 345-kV line.[34]

At 15:42 EDT, FE's western transmission operator informed FE's IT staff that the EMS system functionality was compromised. "Nothing seems to be updating on the computers…. We've had people calling and reporting trips and nothing seems to be updating in the event summary… I think we've got something seriously sick." This is the first evidence that a member of FE's control room staff recognized any aspect of their degraded EMS system. There is no indication that he informed any of the other operators at this moment. However, FE's IT staff discussed the subsequent EMS alarm corrective action with some control room staff shortly thereafter.

Also at 15:42 EDT, the Perry plant operator called back with more evidence of problems. "I'm still getting a lot of voltage spikes and swings on the generator…. I don't know how much longer we're going to survive."[35]

At 15:45 EDT, the tree trimming crew reported that they had witnessed a tree-caused fault on the Eastlake-Juniper 345-kV line; however, the actual fault was on the Hanna-Juniper 345-kV line in the same vicinity. This information added to the confusion in the FE control room, because the operator had indication of flow on the Eastlake-Juniper line.[36]

After the Star-South Canton 345-kV line tripped a third time and locked out at 15:42 EDT, AEP called FE at 15: 45 EDT to discuss and inform them that they had additional lines that showed overload. FE recognized then that the Star breakers had tripped and remained open.[37]

At 15:46 EDT the Perry plant operator called the FE control room a third time to say that the unit was close to tripping off: "It's not looking good…. We ain't going to be here much longer and you're going to have a bigger problem."[38]

At 15:48 EDT, an FE transmission operator sent staff to man the Star substation, and then at 15:50 EDT, requested staffing at the regions, beginning with Beaver, then East Springfield.[39]

At 15:48 EDT, PJM called MISO to report the Star-South Canton trip, but the two reliability coordinators' measures of the resulting line flows on FE's Sammis-Star 345-kV line did not match, causing them to wonder whether the Star-South Canton 345-kV line had returned to service.[40]

At 15:56 EDT, because PJM was still concerned about the impact of the Star-South Canton trip, PJM called FE to report that Star-South Canton had tripped and that PJM thought FE's Sammis-Star line was in actual emergency limit overload. FE could not confirm this overload. FE informed PJM that Hanna-Juniper was also out service. FE believed that the problems existed beyond their system. "AEP must have lost some major stuff."[41]

Emergency Action

For FirstEnergy, as with many utilities, emergency awareness is often focused on energy shortages. Utilities have plans to reduce loads under these circumstances to increasingly greater degrees. Tools include calling for contracted customer load reductions, then public appeals, voltage reductions, and finally shedding system load by cutting

off interruptible and firm customers. FE has a plan for this that is updated yearly. While they can trip loads quickly where there is SCADA control of load breakers (although FE has few of these), from an energy point of view, the intent is to be able to regularly rotate what loads are not being served, which requires calling personnel out to switch the various groupings in and out. This event was not, however, a capacity or energy emergency or system instability, but an emergency due to transmission line overloads.

To handle an emergency effectively a dispatcher must first identify the emergency situation and then determine effective action. AEP identified potential contingency overloads at 15:36 EDT and called PJM even as Star-South Canton, one of the AEP/FE lines they were discussing, tripped and pushed FE's Sammis-Star 345-kV line to its emergency rating. Since that event was the opposite of the focus of their discussion about a TLR for a possible loss of Sammis-Star that would overload Star-South Canton, they recognized that a serious problem had arisen on the system for which they did not have a ready solution.[42] Later, around 15:50 EDT, their conversation reflected emergency conditions (138-kV lines were tripping and several other lines overloaded) but they still found no practical way to mitigate these overloads across utility and reliability coordinator boundaries.

At the control area level, FE remained unaware of the precarious condition their system was in, with key lines out of service, degrading voltages, and severe overloads on their remaining lines.[43] Transcripts show that FE operators were aware of falling voltages and customer problems after loss of the Hanna-Juniper 345-kV line (at 15:32 EDT). They called out personnel to staff substations because they did not think they could see them with their data gathering tools. They were also talking to customers. But there is no indication that FE's operators clearly identified their situation as a possible emergency until around 15:45 EDT when the shift supervisor informed his manager that it looked as if they were losing the system; even then, although FE had grasped that its system was in trouble, it never officially declared that it was an emergency condition and that emergency or extraordinary action was needed.

FE's internal control room procedures and protocols did not prepare them adequately to identify and react to the August 14 emergency. Throughout the afternoon of August 14 there were many clues that FE had lost both its critical monitoring alarm functionality and that its transmission system's reliability was becoming progressively more compromised. However, FE did not fully piece these clues together until after it had already lost critical elements of its transmission system and only minutes before subsequent trippings triggered the cascade phase of the blackout. The clues to a compromised EMS alarm system and transmission system came from a number of reports from various parties external to the FE transmission control room. Calls from FE customers, generators, AEP, MISO and PJM came into the FE control room. In spite of these clues, because of a number of related factors, FE failed to identify the emergency that it faced.

The most critical factor delaying the assessment and synthesis of the clues was a lack of information sharing between the FE system operators. In interviews with the FE operators and analysis of phone transcripts, it is evident that rarely were any of the critical clues shared with fellow operators. This lack of information sharing can be attributed to:

1. Physical separation of operators (the reliability operator responsible for voltage schedules is across the hall from the transmission operators).
2. The lack of a shared electronic log (visible to all), as compared to FE's practice of separate hand-written logs.[44]
3. Lack of systematic procedures to brief incoming staff at shift change times.
4. Infrequent training of operators in emergency scenarios, identification and resolution of bad data, and the importance of sharing key information throughout the control room.

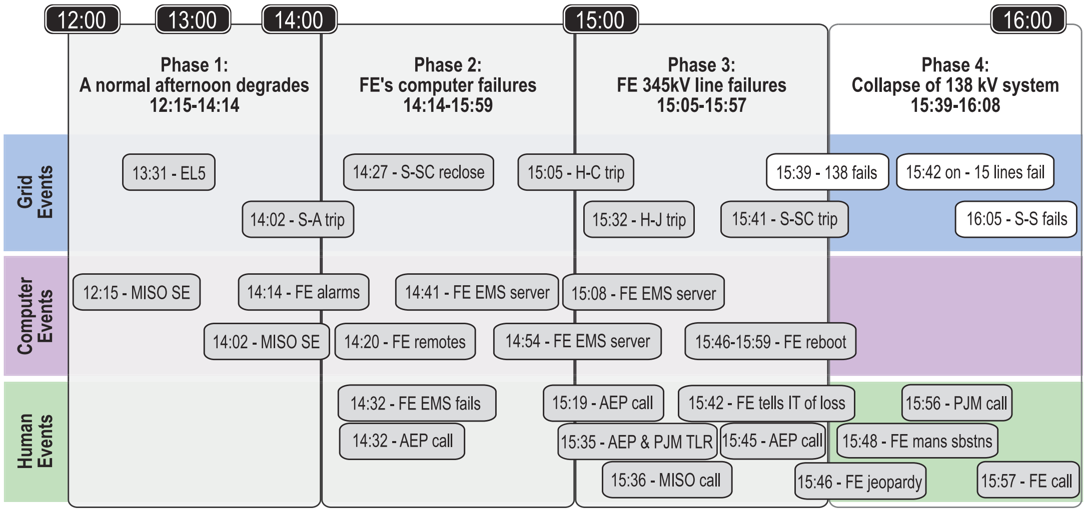
Cause 1: Inadequate Situational Awareness

FE has specific written procedures and plans for dealing with resource deficiencies, voltage depressions, and overloads, and these include instructions to adjust generators and trip firm loads. After the loss of the Star-South Canton line, voltages were below limits, and there were severe line overloads. But FE did not follow any of these procedures on August 14, because FE did not know for most of that time that its system might need such treatment.

Cause 3: Inadequate RC Diagnostic Support

MISO was hindered because it lacked clear visibility, responsibility, authority, and ability to take the actions needed in this circumstance. MISO had interpretive and operational tools and a large amount of

Figure 4.13. Timeline Phase 4



system data, but had a limited view of FE's system. In MISO's function as FE's reliability coordinator, its primary task was to initiate and implement TLRs, recognize and solve congestion problems in less dramatic reliability circumstances with longer solution time periods than those which existed on August 14.

What training did the operators and reliability coordinators have for recognizing and responding to emergencies? FE relied upon on-the-job experience as training for its operators in handling the routine business of a normal day but had never experienced a major disturbance and had no simulator training or formal preparation for recognizing and responding to emergencies. Although all affected FE and MISO operators were NERC certified, neither group had significant training, documentation, or actual experience for how to handle an emergency of this type and magnitude.

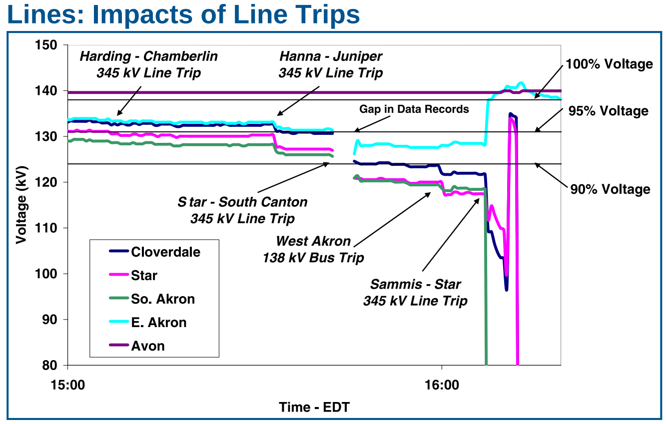
Throughout August 14, most major elements of FE's EMS were working properly. The system was automatically transferring accurate real-time information about FE's system conditions to computers at AEP, MISO, and PJM. FE's operator did not believe the transmission line failures reported by AEP and MISO were real until 15:42 EDT, after FE conversations with the AEP and MISO control rooms and calls from FE IT staff to report the failure of their alarms. At that point in time, FE operators began to think that their system might be in jeopardy—but they did not act to restore any of the lost transmission lines, clearly alert their reliability coordinator or neighbors about their situation, or take other possible remedial measures (such as load-shedding) to stabilize their system.

Phase 4: 138-kV Transmission System Collapse in Northern Ohio: 15:39 to 16:08 EDT

Overview of This Phase

As each of FE's 345-kV lines in the Cleveland area tripped out, it increased loading and decreased voltage on the underlying 138-kV system serving Cleveland and Akron, pushing those lines into overload. Starting at 15:39 EDT, the first of an eventual sixteen 138-kV lines began to fail. Figure 4.14 shows how actual voltages declined at key 138-kV buses as the 345- and 138-kV lines were lost. As these lines failed, the voltage drops caused a number of large industrial customers with voltage-sensitive equipment to go off-line automatically to protect their operations. As the 138-kV lines opened, they blacked out customers in

Figure 4.14. Voltages on FirstEnergy's 138-kV Lines: Impacts of Line Trips



Akron and the areas west and south of the city, ultimately dropping about 600 MW of load.

Key Phase 4 Events

Between 15:39 EDT and 15:58:47 EDT seven 138-kV lines tripped:

4A) 15:39:17 EDT: Pleasant Valley-West Akron 138-kV line tripped and reclosed at both ends.

15:42:05 EDT: Pleasant Valley-West Akron 138-kV West line tripped and reclosed.

15:44:40 EDT: Pleasant Valley-West Akron 138-kV West line tripped and locked out.

4B) 15:42:49 EDT: Canton Central-Cloverdale 138-kV line tripped and reclosed.

15:45:39 EDT: Canton Central-Cloverdale 138-kV line tripped and locked out.

4C) 15:42:53 EDT: Cloverdale-Torrey 138-kV line tripped.

4D) 15:44:12 EDT: East Lima-New Liberty 138-kV line tripped.

4E) 15:44:32 EDT: Babb-West Akron 138-kV line and locked out.

4F) 15:51:41 EDT: East Lima-N. Findlay 138-kV line tripped and reclosed at East Lima end only.

4G) 15:58:47 EDT: Chamberlin-West Akron 138-kV line tripped.

Note: 15:51:41 EDT: Fostoria Central-N. Findlay 138-kV line tripped and reclosed, but never locked out.

At 15:59:00 EDT, the loss of the West Akron bus caused another five 138-kV lines to trip:

4H) 15:59:00 EDT: West Akron 138-kV bus tripped, and cleared bus section circuit breakers at West Akron 138 kV.

4I) 15:59:00 EDT: West Akron-Aetna 138-kV line opened.

4J) 15:59:00 EDT: Barberton 138-kV line opened at West Akron end only. West Akron-B18 138-kV tie breaker opened, affecting West Akron 138/12-kV transformers #3, 4 and 5 fed from Barberton.

4K) 15:59:00 EDT: West Akron-Granger-Stoney-Brunswick-West Medina opened.

4L) 15:59:00 EDT: West Akron-Pleasant Valley 138-kV East line (Q-22) opened.

4M) 15:59:00 EDT: West Akron-Rosemont-Pine-Wadsworth 138-kV line opened.

From 16:00 EDT to 16:08:59 EDT, four 138-kV lines tripped, and the Sammis-Star 345-kV line tripped on overload:

4N) 16:05:55 EDT: Dale-West Canton 138-kV line tripped at both ends, reclosed at West Canton only

4O) 16:05:57 EDT: Sammis-Star 345-kV line tripped

4P) 16:06:02 EDT: Star-Urban 138-kV line tripped

4Q) 16:06:09 EDT: Richland-Ridgeville-Napoleon-Stryker 138-kV line tripped and locked out at all terminals

4R) 16:08:58 EDT: Ohio Central-Wooster 138-kV line tripped

Note: 16:08:55 EDT: East Wooster-South Canton 138-kV line tripped, but successful automatic reclosing restored this line.

4A-G) Pleasant Valley to Chamberlin-West Akron Line Outages

From 15:39 EDT to 15:58:47 EDT, seven 138-kV lines in northern Ohio tripped and locked out. At 15:45:41 EDT, Canton Central-Tidd 345-kV line tripped and reclosed at 15:46:29 EDT because Canton Central 345/138-kV CB "A1" operated multiple times, causing a low air pressure problem that inhibited circuit breaker tripping. This event forced the Canton Central 345/138-kV transformers to disconnect and remain out of service, further weakening the Canton-Akron area 138-kV transmission system. At 15:58:47 EDT the Chamberlin-West Akron 138-kV line tripped.

4H-M) West Akron Transformer Circuit Breaker Failure and Line Outages

At 15:59 EDT FE's West Akron 138-kV bus tripped due to a circuit breaker failure on West Akron transformer #1. This caused the five remaining 138-kV lines connected to the West Akron substation to open. The West Akron 138/12-kV transformers remained connected to the Barberton-West Akron 138-kV line, but power flow to West Akron 138/69-kV transformer #1 was interrupted.

4N-O) Dale-West Canton 138-kV and Sammis-Star 345-kV Lines Tripped

After the Cloverdale-Torrey line failed at 15:42 EDT, Dale-West Canton was the most heavily loaded line on FE's system. It held on, although heavily overloaded to 160 and 180% of normal

ratings, until tripping at 16:05:55 EDT. The loss of this line had a significant effect on the area, and voltages dropped significantly. More power shifted back to the remaining 345-kV network, pushing Sammis-Star's loading above 120% of rating. Two seconds later, at 16:05:57 EDT, Sammis-Star tripped out. Unlike the previous three 345-kV lines, which tripped on short circuits to ground due to tree contacts, Sammis-Star tripped because its protective relays saw low apparent impedance (depressed voltage divided by abnormally high line current)—i.e., the relay reacted as if the high flow was due to a short circuit. Although three more 138-kV lines dropped quickly in Ohio following the Sammis-Star trip, loss of the Sammis-Star line marked the turning point at which system problems in northeast Ohio initiated a cascading blackout across the northeast United States and Ontario.[45]

Losing the 138-kV System

The tripping of 138-kV transmission lines that began at 15:39 EDT occurred because the loss of the combination of the Harding-Chamberlin, Hanna-Juniper and Star-South Canton 345-kV lines overloaded the 138-kV system with electricity flowing north toward the Akron and Cleveland loads. Modeling indicates that the return of either the Hanna-Juniper or Chamberlin-Harding 345-kV lines would have diminished, but not alleviated, all of the 138-kV overloads. In theory, the return of both lines would have restored all the 138 lines to within their emergency ratings.

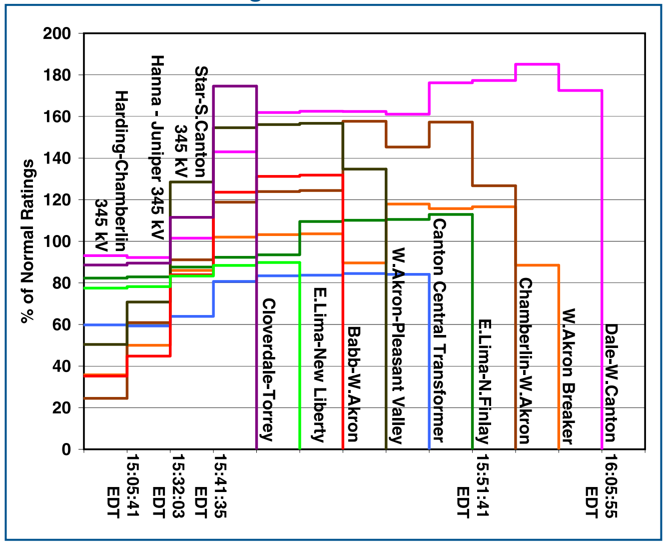
Cause 1: Inadequate Situational Awareness

However, all three 345-kV lines had already been compromised due to tree contacts so it is unlikely that FE would have successfully restored either line had they known it had tripped out, and since Star-South Canton had already tripped and reclosed three times it is also unlikely that an operator knowing this would have trusted it to operate securely under emergency conditions. While generation redispatch scenarios alone would not have solved the overload problem, modeling indicates that shedding load in the Cleveland and Akron areas may have reduced most line loadings to within emergency range and helped stabilize the system. However, the amount of load shedding required grew rapidly as FE's system unraveled.

Loss of the Sammis-Star 345-kV Line

Figure 4.15, derived from investigation team modeling, shows how the power flows shifted across FE's 345- and key 138-kV northeast Ohio lines as the line failures progressed. All lines were loaded within normal limits after the Harding-Chamberlin lock-out, but after the Hanna-Juniper trip at 15:32, the Star-South Canton 345-kV line and three 138-kV lines jumped above normal loadings. After Star-South Canton locked out at 15:41 EDT, five 138-kV and the Sammis-Star 345-kV lines were overloaded and Star-South Canton was within its emergency rating. From that point, as the graph shows, each subsequent line loss increased loadings on other lines, some loading to well over 150% of normal ratings before they failed. The Sammis-Star 345-kV line stayed in service until it tripped at 16:05:57 EDT.

Figure 4.15. Simulated Effect of Prior Outages on 138-kV Line Loadings



Endnotes

[1] *August 14, 2003 Outage Sequence of Events*, U.S./Canada Power Outage Task Force (September 12, 2003), http://www.electricity.doe.gov/documents/1282003113351_BlackoutSummary.pdf.

[2] DOE Site Visit to FE 10/8/2003: Steve Morgan.

[3] DOE Site Visit to FE, September 3, 2003, Hough interview: "When asked whether the voltages seemed unusual, he said that some sagging would be expected on a hot day, but on August 14th the voltages did seem unusually low." Spidle interview: "The voltages for the day were not particularly bad."

[4] Manual of Operations, valid as of March 3, 2003, Process flowcharts: Voltage Control and Reactive Support – Plant and System Voltage Monitoring Under Normal Conditions.

[5] 14:13:18. Channel 16 - Sammis 1. 13:15:49 / Channel 16 – West Lorain (FE Reliability Operator (RO) says, "Thanks. We're starting to sag all over the system.") / 13:16:44. Channel 16 – Eastlake (talked to two operators) (RO says, "We got a way bigger load than we thought we would have." And "…So we're starting to sag all over the system.") / 13:20:22. Channel 16 – RO to "Berger" / 13:22:07. Channel 16 – "control room"

RO says, "We're sagging all over the system. I need some help." / 13:23:24. Channel 16 – "Control room, Tom" / 13:24:38. Channel 16 – "Unit 9" / 13:26:04. Channel 16 – "Dave" / 13:28:40. Channel 16 "Troy Control". Also general note in RO Dispatch Log.

[6]Example at 13:33:40, Channel 3, FE transcripts.

[7]Investigation Team Site Visit to MISO, Walsh and Seidu interviews.

[8]FE had and ran a state estimator every 30 minutes. This served as a base from which to perform contingency analyses. FE's contingency analysis tool used SCADA and EMS inputs to identify any potential overloads that could result from various line or equipment outages. FE indicated that it has experienced problems with the automatic contingency analysis operation since the system was installed in 1995. As a result, FE operators or engineers ran contingency analysis manually rather than automatically, and were expected to do so when there were questions about the state of the system. Investigation team interviews of FE personnel indicate that the contingency analysis model was likely running but not consulted at any point in the afternoon of August 14.

[9]After the Stuart-Atlanta line tripped, Dayton Power & Light did not immediately provide an update of a change in equipment availability using a standard form that posts the status change in the SDX (System Data Exchange, the NERC database which maintains real-time information on grid equipment status), which relays that notice to reliability coordinators and control areas. After its state estimator failed to solve properly, MISO checked the SDX to make sure that they had properly identified all available equipment and outages, but found no posting there regarding Stuart-Atlanta's outage.

[10]Investigation team field visit, interviews with FE personnel on October 8-9, 2003.

[11] DOE Site Visit to First Energy, September 3, 2003, Interview with David M. Elliott.

[12]FE Report, "Investigation of FirstEnergy's Energy Management System Status on August 14, 2003", Bullet 1, Section 4.2.11.

[13]Investigation team interviews with FE, October 8-9, 2003.

[14]DOE Site Visit at FE, October 8-9, 2003; investigation team was advised that FE had discovered this effect during post-event investigation and testing of the EMS. FE's report "Investigation of FirstEnergy's Energy Management System Status on August 14, 2003" also indicates that this finding was "verified using the strip charts from 8-14-03" (page 23), not that the investigation of this item was instigated by operator reports of such a failure.

[15] There is a conversation between a Phil and a Tom that speaks of "flatlining" 15:01:33. Channel 15. There is no mention of AGC or generation control in the DOE Site Visit interviews with the reliability coordinator.

[16]DOE Site Visit to FE, October 8-9, 2003, Sanicky Interview: "From his experience, it is not unusual for alarms to fail. Often times, they may be slow to update or they may die completely. From his experience as a real-time operator, the fact that the alarms failed did not surprise him." Also from same document, Mike McDonald interview "FE has previously had [servers] down at the same time. The big issue for them was that they were not receiving new alarms."

[17] A "cold" reboot of the XA21 system is one in which all nodes (computers, consoles, etc.) of the system are shut down and then restarted. Alternatively, a given XA21 node can be "warm" rebooted wherein only that node is shut down and restarted, or restarted from a shutdown state. A cold reboot will take significantly longer to perform than a warm one. Also during a cold reboot much more of the system is unavailable for use by the control room operators for visibility or control over the power system. Warm reboots are not uncommon, whereas cold reboots are rare. All reboots undertaken by FE's IT EMSS support personnel on August 14 were warm reboots.

[18]The cold reboot was done in the early morning of 15 August and corrected the alarm problem as hoped.

[19]Example at 14:19, Channel l4, FE transcripts.

[20]Example at 14:25, Channel 8, FE transcripts.

[21]Example at 14:32, Channel 15, FE transcripts.

[22] Investigation team transcript, meeting on September 9, 2003, comments by Mr. Steve Morgan, Vice President Electric Operations:

Mr. Morgan: The sustained outage history for these lines, 2001, 2002, 2003, up until the event, Chamberlin-Harding had zero operations for those two-and-a-half years. And Hanna-Juniper had six operations in 2001, ranging from four minutes to maximum of 34 minutes. Two were unknown, one was lightning, one was a relay failure, and two were really relay scheme mis-operations. They're category other. And typically, that—I don't know what this is particular to operations, that typically occurs when there is a mis-operation.

Star-South Canton had no operations in that same period of time, two-and-a-half years. No sustained outages. And Sammis-Star, the line we haven't talked about, also no sustained outages during that two-and-a-half year period.

So is it normal? No. But 345 lines do operate, so it's not unknown.

[23] "Interim Report, Utility Vegetation Management," U.S.-Canada Joint Outage Investigation Task Force, Vegetation Management Program Review, October 2003, page 7.

[24] Investigation team October 2, 2003, fact-finding meeting, Steve Morgan statement.

[25] "FE MISO Findings," page 11.

[26]FE was conducting right-of-way vegetation maintenance on a 5-year cycle, and the tree crew at Hanna-Juniper was three spans away, clearing vegetation near the line, when the contact occurred on August 14. Investigation team 9/9/03 meeting transcript, and investigation field team discussion with the tree-trimming crew foreman.

[27] Based on "FE MISO Findings" document, page 11.

[28] "Interim Report, Utility Vegetation Management," US-Canada Joint Outage Task Force, Vegetation Management Program Review, October 2003, page 6.

[29]Investigation team September 9, 2003 meeting transcripts, Mr. Steve Morgan, First Energy Vice President, Electric System Operations:

Mr. Benjamin: Steve, just to make sure that I'm understanding it correctly, you had indicated that once after Hanna-Juniper relayed out, there wasn't really a problem with voltage on the system until Star-S. Canton operated. But were the system operators aware that when Hanna-Juniper was out, that if Star-S. Canton did trip, they would be outside of operating limits?

Mr. Morgan: I think the answer to that question would have required a contingency analysis to be done probably on demand for that operation. It doesn't appear to me that a contingency analysis, and certainly not a demand contingency analysis, could have been run in that period of time. Other than experience, I don't know that they would have been able

to answer that question. And what I know of the record right now is that it doesn't appear that they ran contingency analysis on demand.

Mr. Benjamin: Could they have done that?

Mr. Morgan: Yeah, presumably they could have.

Mr. Benjamin: You have all the tools to do that?

Mr. Morgan: They have all the tools and all the information is there. And if the State Estimator is successful in solving, and all the data is updated, yeah, they could have. I would say in addition to those tools, they also have access to the planning load flow model that can actually run the same—full load of the model if they want to.

30 Example synchronized at 14:32 (from 13:32) #18 041 TDC-E2 283.wav, AEP transcripts.

31 Example synchronized at 14:19 #2 020 TDC-E1 266.wav, AEP transcripts.

32 Example at 15:36 Channel 8, FE transcripts.

33 Example at 15:41:30 Channel 3, FE transcripts.

34 Example synchronized at 15:36 (from 14:43) Channel 20, MISO transcripts.

35 Example at 15:42:49, Channel 8, FE transcripts.

36 Example at 15:46:00, Channel 8 FE transcripts.

37 Example at 15:45:18, Channel 4, FE transcripts.

38 Example at 15:46:00, Channel 8 FE transcripts.

39 Example at 15:50:15, Channel 12 FE transcripts.

40 Example synchronized at 15:48 (from 14:55), channel 22, MISO transcripts.

41 Example at 15:56:00, Channel 31, FE transcripts.

42 AEP Transcripts CAE1 8/14/2003 14:35 240.

43 FE Transcripts 15:45:18 on Channel 4 and 15:56:49 on Channel 31.

44 The operator logs from FE's Ohio control center indicate that the west desk operator knew of the alarm system failure at 14:14, but that the east desk operator first knew of this development at 15:45. These entries may have been entered after the times noted, however.

45 The investigation team determined that FE was using a different set of line ratings for Sammis-Star than those being used in the MISO and PJM reliability coordinator calculations or by its neighbor AEP. Specifically, FE was operating Sammis-Star assuming that the 345-kV line was rated for summer normal use at 1,310 MVA, with a summer emergency limit rating of 1,310 MVA. In contrast, MISO, PJM and AEP were using a more conservative rating of 950 MVA normal and 1,076 MVA emergency for this line. The facility owner (in this case FE) is the entity which provides the line rating; when and why the ratings were changed and not communicated to all concerned parties has not been determined.

5. The Cascade Stage of the Blackout

Chapter 4 described how uncorrected problems in northern Ohio developed to a point that a cascading blackout became inevitable. However, the Task Force's investigation also sought to understand how and why the cascade spread and stopped as it did. As detailed below, the investigation determined the sequence of events in the cascade, and in broad terms how it spread and how it stopped in each general geographic area.[1]

Why Does a Blackout Cascade?

Major blackouts are rare, and no two blackout scenarios are the same. The initiating events will vary, including human actions or inactions, system topology, and load/generation balances. Other factors that will vary include the distance between generating stations and major load centers, voltage profiles, and the types and settings of protective relays in use.

Most wide-area blackouts start with short circuits (faults) on several transmission lines in short succession—sometimes resulting from natural causes such as lightning or wind or, as on August 14, resulting from inadequate tree management in right-of-way areas. A fault causes a high current and low voltage on the line containing the fault. A protective relay for that line detects the high current and low voltage and quickly trips the circuit breakers to isolate that line from the rest of the power system.

A cascade occurs when there is a sequential tripping of numerous transmission lines and generators in a widening geographic area. A cascade can be triggered by just a few initiating events, as was seen on August 14. Power swings and voltage fluctuations caused by these initial events can cause other lines to detect high currents and low voltages that appear to be faults, even when faults do not actually exist on those other lines. Generators are tripped off during a cascade to protect them from severe power and voltage swings. Relay protection systems work well to protect lines and generators from damage and to isolate them from the system under normal, steady conditions. However, when power system operating and design criteria are violated as a result of several outages occurring at the same time, most common protective relays cannot distinguish between the currents and voltages seen in a system cascade from those caused by a fault. This leads to more and more lines and generators being tripped, widening the blackout area.

How Did the Cascade Evolve on August 14?

At 16:05:57 Eastern Daylight Time, the trip and lock-out of FE's Sammis-Star 345 kV line set off a cascade of interruptions on the high voltage system, causing electrical fluctuations and facility trips as within seven minutes the blackout rippled from the Akron area across much of the northeast United States and Canada. By 16:13 EDT, more than 263 power plants (531 individual generating units) had been lost, and tens of millions of people in the United States and Canada were without electric power.

Chapter 4 described the four phases that led to the initiation of the cascade at about 16:06 EDT. After 16:06 EDT, the cascade evolved in three distinct phases:

- **Phase 5.** The collapse of FE's transmission system induced unplanned power surges across the region. Shortly before the collapse, large electricity flows were moving across FE's system from generators in the south (Tennessee, Kentucky, Missouri) to load centers in northern Ohio, eastern Michigan, and Ontario. This pathway in northeastern Ohio became unavailable with the collapse of FE's transmission system. The electricity then took alternative paths to the load centers located along the shore of Lake Erie. Power surged in from western Ohio and Indiana on one side and from Pennsylvania through New York and Ontario around the northern side of Lake Erie. Transmission lines in these areas, however, were already heavily loaded with normal flows, and some of them began to trip.

- **Phase 6.** The northeast then separated from the rest of the Eastern Interconnection due to these additional power surges. The power surges resulting from the FE system failures caused lines in neighboring areas to see overloads that caused impedance relays to operate. The result was a wave of line trips through western Ohio that separated AEP from FE. Then the line trips progressed northward into Michigan separating western and eastern Michigan.

  With paths cut from the west, a massive power surge flowed from PJM into New York and Ontario in a counter-clockwise flow around Lake Erie to serve the load still connected in eastern Michigan and northern Ohio. The relays on the lines between PJM and New York saw this massive power surge as faults and tripped those lines. Lines in western Ontario also became overloaded and tripped. The entire northeastern United States and the province of Ontario then became a large electrical island separated from the rest of the Eastern Interconnection. This large island, which had been importing power prior to the cascade, quickly became unstable as there was not sufficient generation in operation within it to meet electricity demand. Systems to the south and west of the split, such as PJM, AEP and others further away remained intact and were mostly unaffected by the outage. Once the northeast split from the rest of the Eastern Interconnection, the cascade was isolated.

Phase 7. In the final phase, the large electrical island in the northeast was deficient in generation and unstable with large power surges and swings in frequency and voltage. As a result, many lines and generators across the disturbance area tripped, breaking the area into several electrical islands. Generation and load within these smaller islands was often unbalanced, leading to further tripping of lines and generating units until equilibrium was established in each island. Although much of the disturbance area was fully blacked out in this process, some islands were able to reach equilibrium without total loss of service. For example, most of New England was stabilized and generation and load restored to balance. Approximately half of the generation and load remained on in western New York, which has an abundance of generation. By comparison, other areas with large load centers and insufficient generation nearby to meet that load collapsed into a blackout condition (Figure 5.1).

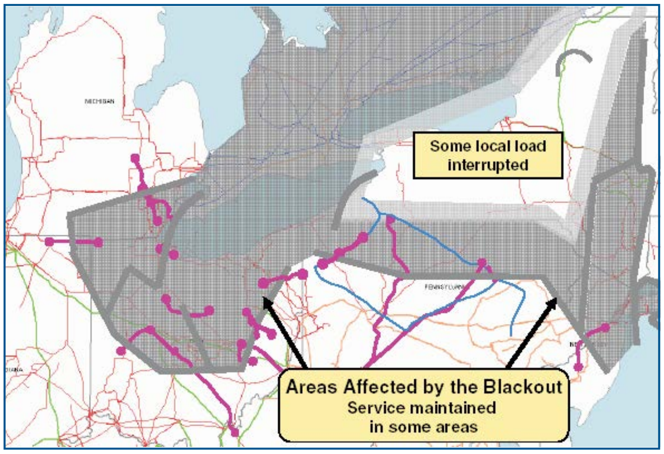
Impedance Relays

The most common protective device for transmission lines is the impedance relay (also known as a distance relay). It detects changes in currents and voltages to determine the apparent impedance of the line. A relay is installed at each end of a transmission line. Each relay is actually three relays within one, with each element looking at a particular "zone" or length of the line being protected.

- The first zone looks for faults on the line itself, with no intentional delay.
- The second zone is set to look at the entire line and slightly beyond the end of the line with a slight time delay. The slight delay on the zone 2 relay is useful when a fault occurs near one end of the line. The zone 1 relay near that end operates quickly to trip the circuit breakers on that end. However, the zone 1 relay on the far end may not be able to tell if the fault is just inside the line or just beyond the line. In this case, the zone 2 relay on the far end trips the breakers after a short delay, allowing the zone 1 relay near the fault to open the line on that end first.
- The third zone is slower acting and looks for faults well beyond the length of the line. It can be thought of as a backup, but would generally not be used under normal conditions.

An impedance relay operates when the apparent impedance, as measured by the current and voltage seen by the relay, falls within any one of the operating zones for the appropriate amount of time for that zone. The relay will trip and cause circuit breakers to operate and isolate the line. Typically, Zone 1 and 2 operations are used to protect lines from faults. Zone 3 relay operations, as in the August 14 cascade, can occur if there are apparent faults caused by large swings in voltages and currents.

Figure 5.1. Area Affected by the Blackout



What Stopped the August 14 Blackout from Cascading Further?

The investigation concluded that one or more of the following likely determined where and when the cascade stopped spreading:

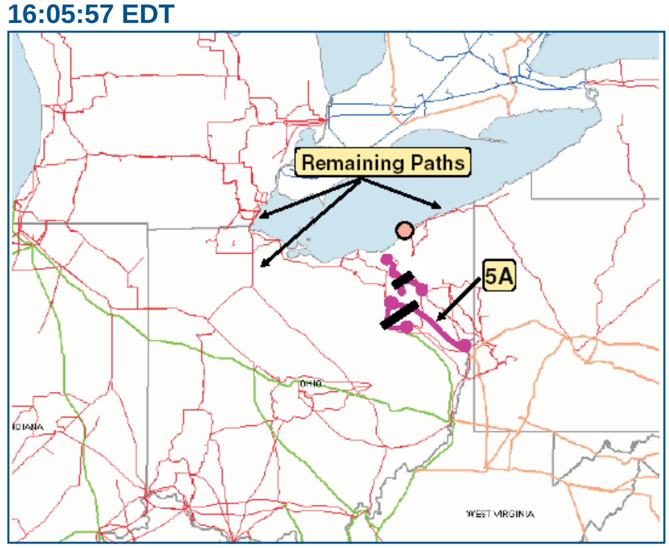
- The effects of a disturbance travel over power lines and become dampened the further they are from the initial point, much like the ripple from a stone thrown in a pond. Thus, the voltage and current swings seen by relays on lines farther away from the initial disturbance are not as severe, and at some point they are no longer sufficient to induce lines to trip.
- Higher voltage lines and more densely networked lines, such as the 500-kV system in PJM and the 765-kV system in AEP, are better able to absorb voltage and current swings and thus serve as a barrier to the spreading of a cascade. As seen in Phase 6, the cascade progressed into western Ohio and then northward through Michigan through the areas that had the fewest transmission lines. Because there were fewer lines, each line absorbed more of the power and voltage surges and was more vulnerable to tripping. A similar effect was seen toward the east as the lines between New York and Pennsylvania, and eventually northern New Jersey tripped. The cascade of transmission line outages became isolated after the northeast United States and Ontario were completely separated from the rest of the Eastern Interconnection and no more power flows were possible into the northeast (except the DC ties from Quebec, which continued to supply power to western New York and New England).
- Some areas, due to line trips, were isolated from the portion of the grid that was experiencing instability. Many of these areas retained sufficient on-line generation or the capacity to import power from other parts of the grid, unaffected by the surges or instability, to meet demand. As the cascade progressed, and more generators and lines tripped off to protect themselves from severe damage, and some areas completely separated from the unstable part of the Eastern Interconnection. In many of these areas there was sufficient generation to stabilize the system. After the large island was formed in the northeast, symptoms of frequency and voltage collapse became evident. In some parts of the large area, the system was too unstable and shut itself down. In other parts, there was sufficient generation, coupled with fast-acting automatic load shedding, to stabilize frequency and voltage. In this manned, most of New England remained energized. Approximately half of the generation and load remained on in western New York, aided by generation in southern Ontario that split and stayed with western New York. There were other smaller isolated pockets of load and generation that were able to achieve equilibrium and remain energized.

Phase 5: 345-kV Transmission System Cascade in Northern Ohio and South-Central Michigan

Overview of This Phase

This initial phase of the cascade began because after the loss of FE's Sammis-Star 345-kV line and the underlying 138-kV system, there were no large transmission paths left from the south to support the significant amount of load in northern Ohio (Figure 5.2). This placed a significant load burden

Figure 5.2. Sammis-Star 345-kV Line Trip, 16:05:57 EDT



onto the transmission paths north and northwest into Michigan, causing a steady loss of lines and power plants.

Key Events in This Phase

5A) 16:05:57 EDT: Sammis-Star 345-kV tripped.

5B) 16:08:59 EDT: Galion-Ohio Central-Muskingum 345-kV line tripped.

5C) 16:09:06 EDT: East Lima-Fostoria Central 345-kV line tripped, causing major power swings through New York and Ontario into Michigan.

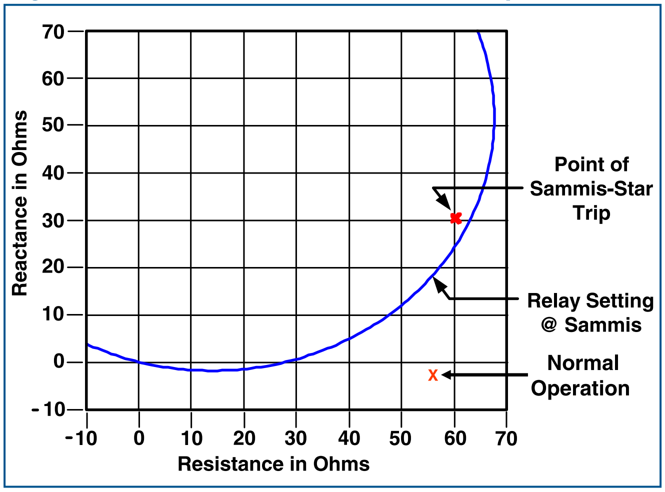
5D) 16:09:08 EDT to 16:10:27 EDT: Several power plants lost, totaling 937 MW.

5A) Sammis-Star 345-kV Tripped: 16:05:57 EDT

Sammis-Star did not trip due to a short circuit to ground (as did the prior 345-kV lines that tripped). Sammis-Star tripped due to protective relay action that measured low apparent impedance (depressed voltage divided by abnormally high line current) (Figure 5.3). There was no fault and no major power swing at the time of the trip—rather, high flows above the line's emergency rating together with depressed voltages caused the overload to appear to the protective relays as a remote fault on the system. In effect, the relay could no longer differentiate between a remote three-phase fault and an exceptionally high line-load condition. Moreover, the reactive flows (VArs) on the line were almost ten times higher than they had been earlier in the day. The relay operated as it was designed to do.

The Sammis-Star 345-kV line trip completely severed the 345-kV path into northern Ohio from southeast Ohio, triggering a new, fast-paced sequence of 345-kV transmission line trips in which each line trip placed a greater flow burden on those lines remaining in service. These line outages left only three paths for power to flow into northern Ohio: (1) from northwest Pennsylvania to northern Ohio around the south shore of Lake Erie, (2) from southern Ohio, and (3) from eastern Michigan and Ontario. The line interruptions substantially weakened northeast Ohio as a source of power to eastern Michigan, making the Detroit area more reliant on 345-kV lines west and northwest of Detroit, and from northwestern Ohio to eastern Michigan.

Figure 5.3. Sammis-Star 345-kV Line Trips



Transmission Lines into Northwestern Ohio Tripped, and Generation Tripped in South Central Michigan and Northern Ohio: 16:08:59 EDT to 16:10:27 EDT

5B) Galion-Ohio Central-Muskingum 345-kV line tripped: 16:08:59 EDT

5C) East Lima-Fostoria Central 345-kV line tripped, causing a large power swing from Pennsylvania and New York through Ontario to Michigan: 16:09:05 EDT

The tripping of the Galion-Ohio Central-Muskingum and East Lima-Fostoria Central 345-kV transmission lines removed the transmission paths from southern and western Ohio into northern Ohio and eastern Michigan. Northern Ohio was connected to eastern Michigan by only three 345-kV transmission lines near the southwestern

System Oscillations

The electric power system constantly experiences small, stable power oscillations. They occur as generator rotors accelerate or slow down while rebalancing electrical output power to mechanical input power, to respond to changes in load or network conditions. These oscillations are observable in the power flow on transmission lines that link generation to load or in the tie lines that link different regions of the system together. The greater the disturbance to the network, the more severe these oscillations can become, even to the point where flows become so great that protective relays trip the connecting lines, just as a rubber band breaks when stretched too far. If the lines connecting different electrical regions separate, each region will drift to its own frequency.

Oscillations that grow in amplitude are called unstable oscillations. Oscillations are also sometimes called power swings, and once initiated they flow back and forth across the system rather like water sloshing in a rocking tub.

bend of Lake Erie. Thus, the combined northern Ohio and eastern Michigan load centers were left connected to the rest of the grid only by: (1) transmission lines eastward from northeast Ohio to northwest Pennsylvania along the southern shore of Lake Erie, and (2) westward by lines west and northwest of Detroit, Michigan and from Michigan into Ontario (Figure 5.4).

The East Lima-Fostoria Central 345-kV line tripped at 16:09:06 EDT due to high currents and low voltage, and the resulting large power swings (measuring about 400 MW when they passed through NYPA's Niagara recorders) marked the moment when the system became unstable. This was the first of several inter-area power and frequency events that occurred over the next two minutes. It was the system's response to the loss of the Ohio-Michigan transmission paths (above), and the stress that the still-high Cleveland, Toledo and Detroit loads put onto the surviving lines and local generators.

In Figure 5.5, a high-speed recording of 345-kV flows past Niagara Falls shows the New York to Ontario power swing, which continued to oscillate for over 10 seconds. The recording shows the magnitude of subsequent flows triggered by the trips of the Hampton-Pontiac and Thetford-Jewell 345-kV lines in Michigan and the Perry-Ashtabula 345-kV line linking the Cleveland area to Pennsylvania. The very low voltages on the northern Ohio transmission system made it very difficult for the generation in the Cleveland and Lake Erie area to maintain synchronization with the Eastern Interconnection. Over the next two minutes, generators in this area shut down after reaching a point of no recovery as the stress level across the remaining ties became excessive.

Before this first major power swing on the Michigan/Ontario interface, power flows in the NPCC Region (Ontario and the Maritimes, New England, New York, and the mid-Atlantic portion of PJM) were typical for the summer period, and well within acceptable limits. Transmission and generation facilities were then in a secure state across the NPCC.

5D) Multiple Power Plants Tripped, Totaling 937 MW: 16:09:08 to 16:10:27 EDT

Michigan Cogeneration Venture plant reduction of 300 MW (from 1,263 MW to 963 MW)

Kinder Morgan units 1 and 2 trip (200 MW total)

Avon Lake 7 unit trips (82 MW)

Berger 3, 4, and 5 units trip (355 MW total)

The Midland Cogeneration Venture (MCV) plant is in central Michigan. Kinder Morgan is in south-central Michigan. The large power reversal caused frequency and voltage fluctuations at the plants. Their automatic control systems responded to these transients by trying to adjust output to raise voltage or respond to the frequency changes, but subsequently tripped off-line. The Avon Lake and Burger units, in or near Cleveland, likely tripped off due to the low voltages prevailing in the Cleveland area and 138-kV line trips near Burger 138-kV substation (northern Ohio) (Figure 5.6).

Power flows into Michigan from Indiana increased to serve loads in eastern Michigan and northern Ohio (still connected to the grid through northwest Ohio and Michigan) and voltages

Figure 5.4. Ohio 345-kV Lines Trip, 16:08:59 to 16:09:07 EDT

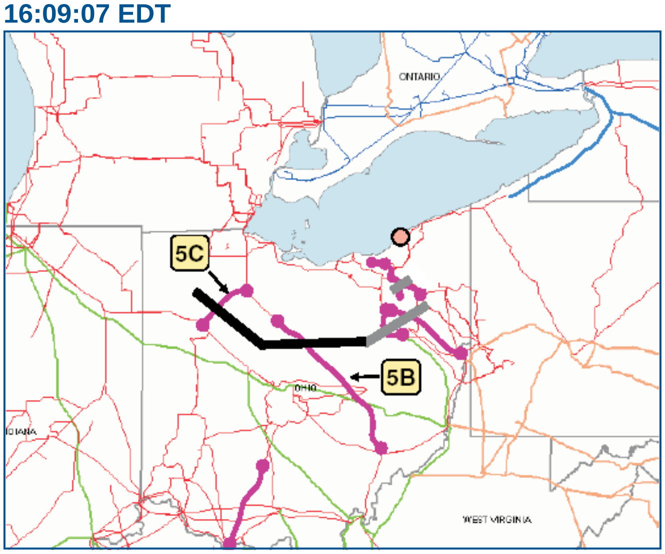
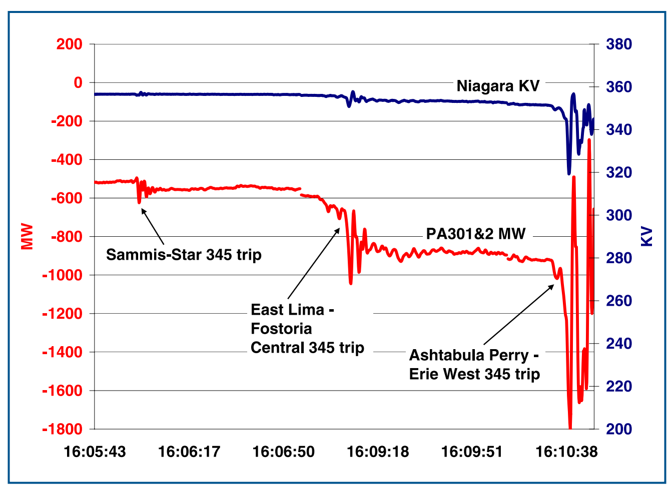


Figure 5.5. New York-Ontario Line Flows at Niagara



Note: Does not include 230-kV line flow.

dropped from the imbalance between high loads and limited transmission and generation capability.

Phase 6: The Full Cascade

Between 16:10:36 EDT and 16:13 EDT, thousands of events occurred on the grid, driven by physics and automatic equipment operations. When it was over, much of the northeast United States and the Canadian province of Ontario was in the dark.

Key Phase 6 Events

Transmission Lines Disconnected Across Michigan and Northern Ohio, Generation Shut Down in Central Michigan and Northern Ohio, and Northern Ohio Separated from Pennsylvania: 16:10:36 EDT to 16:10:39 EDT

6A) Transmission and more generation tripped within Michigan: 16:10:36 EDT to 16:10:37 EDT:

Argenta-Battlecreek 345-kV line tripped

Battlecreek-Oneida 345-kV line tripped

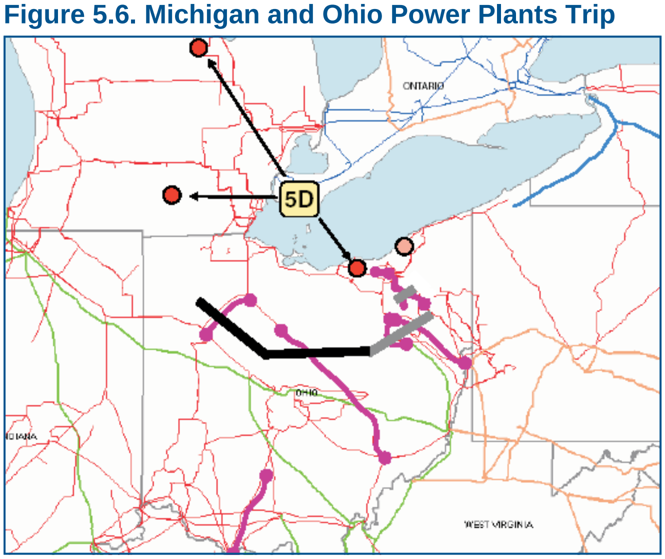
Argenta-Tompkins 345-kV line tripped

Sumpter Units 1, 2, 3, and 4 units tripped (300 MW near Detroit)

MCV Plant output dropped from 944 MW to 109 MW.

Together, the above line outages interrupted the east-to-west transmission paths into the Detroit area from south-central Michigan. The Sumpter generation units tripped in response to under-voltage on the system. Michigan lines northwest of Detroit then began to trip, as noted below (Figure 5.7).

Figure 5.6. Michigan and Ohio Power Plants Trip



6B) More Michigan lines tripped: 16:10:37 EDT to 16:10:38 EDT

Hampton-Pontiac 345-kV line tripped

Thetford-Jewell 345-kV line tripped

These 345-kV lines connect Detroit to the north. When they tripped out of service, it left the loads in Detroit, Toledo, Cleveland, and their surrounding areas served only by local generation and the lines connecting Detroit east to Ontario and Cleveland east to northeast Pennsylvania.

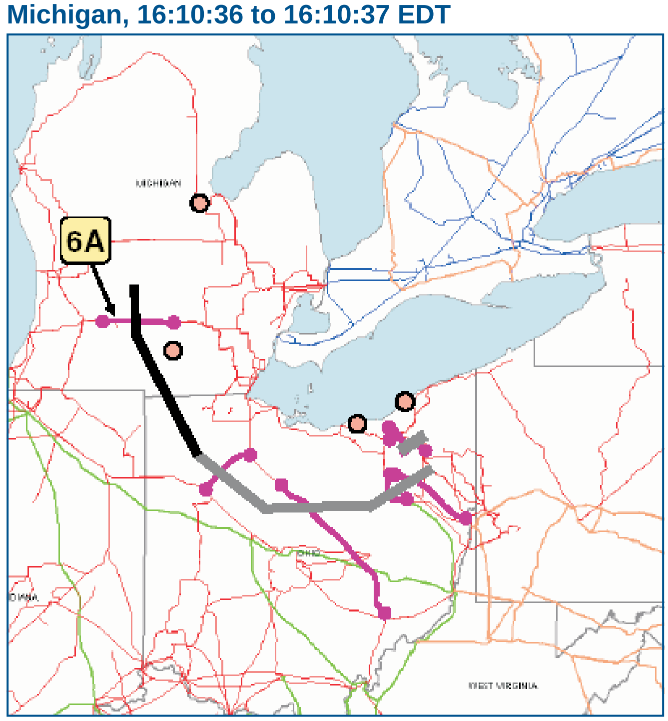
6C) Cleveland separated from Pennsylvania, flows reversed and a huge power surge flowed counter-clockwise around Lake Erie: 16:10:38.6 EDT

Perry-Ashtabula-Erie West 345-kV line tripped: 16:10:38.6 EDT

Large power surge to serve loads in eastern Michigan and northern Ohio swept across Pennsylvania, New Jersey, and New York through Ontario into Michigan: 16:10:38.6 EDT.

Perry-Ashtabula-West Erie was the last 345-kV line connecting northern Ohio to the east. This line's trip separated the Ohio 345-kV transmission system from Pennsylvania. When it tripped, the load centers in eastern Michigan and northern Ohio remained connected to the rest of the Eastern Interconnection only at the interface between the

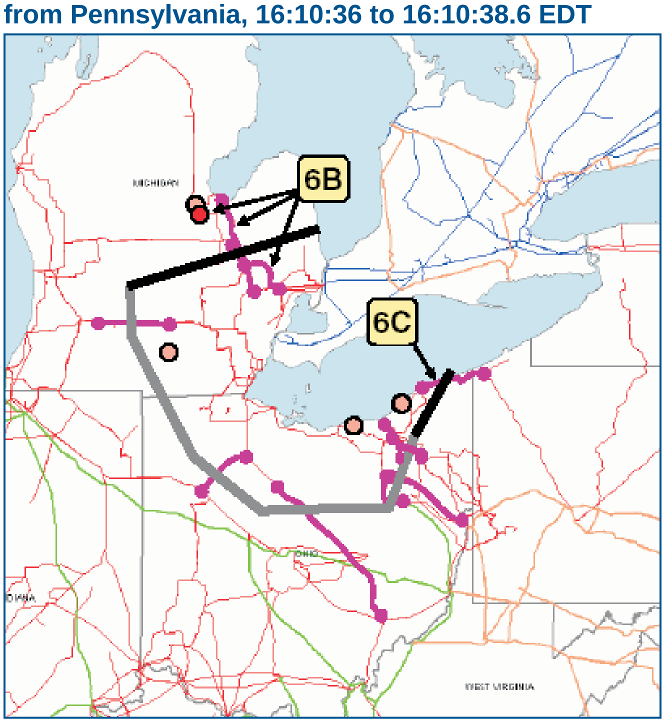
Figure 5.7. Transmission and Generation Trips in Michigan, 16:10:36 to 16:10:37 EDT



Michigan and Ontario systems (Figure 5.8). Eastern Michigan and northern Ohio now had little internal generation left and voltage was declining. Between 16:10:39 EDT and 16:10:50 EDT under-frequency load shedding in the Cleveland area operated and interrupted about 1,750 MW of load. The frequency in the Cleveland area (by then separated from the Eastern Interconnection to the south) was also dropping rapidly and the load shedding was not enough to arrest the frequency decline. Since the electrical system always seeks to balance load and generation, the high loads in Cleveland drew power over the only major transmission path remaining—the lines from eastern Michigan east into Ontario.

Before the loss of the Perry-Ashtabula-West Erie line, 437 MW was flowing from Michigan into Ontario. At 16:10:38.6 EDT, after the other transmission paths into Michigan and Ohio failed, the power that had been flowing over them reversed direction in a fraction of a second. Electricity began flowing toward Michigan via a giant loop through Pennsylvania and into New York and Ontario and then into Michigan via the remaining transmission path. Flows at Niagara Falls 345-kV lines measured over 800 MW, and over 3,500 MW at the Ontario to Michigan interface (Figure 5.9). This sudden large change in power flows drastically lowered voltage and increased current levels on the transmission lines along the Pennsylvania-New York transmission interface.

Figure 5.8. Michigan Lines Trip and Ohio Separates from Pennsylvania, 16:10:36 to 16:10:38.6 EDT

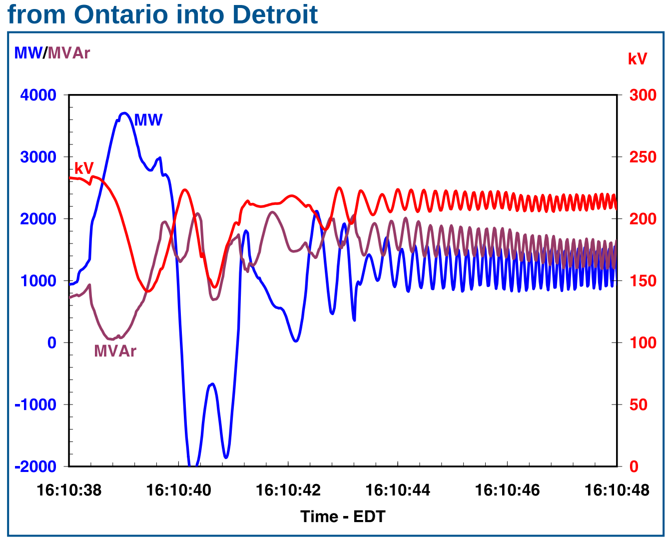


This was a transient frequency swing, so frequency was not the same across the Eastern Interconnection. As Figure 5.8 shows, this frequency imbalance and the accompanying power swing resulted in a rapid rate of voltage decay. Flows into Detroit exceeded 3,500 MW and 1,500 MVAr, meaning that the power surge was draining both active and reactive power out of the northeast to prop up the low voltages in eastern Michigan and Detroit. This magnitude of reactive power draw caused voltages in Ontario and New York to drop. At the same time, local voltages in the Detroit area were low because there was still not enough supply to meet load. Detroit would soon black out (as evidenced by the rapid power swings decaying after 16:10:43 EDT).

Between 16:10:38 and 16:10:41 EDT, the power surge caused a sudden extraordinary increase in system frequency to 60.3 Hz. A series of circuits tripped along the border between PJM and the NYISO due to apparent impedance faults (short circuits). The surge also moved into New England and the Maritimes region of Canada. The combination of the power surge and frequency rise caused 380 MW of pre-selected Maritimes generation to drop off-line due to the operation of the New Brunswick Power "Loss of Line 3001" Special Protection System. Although this system was designed to respond to failure of the 345-kV link between the Maritimes and New England, it operated in response to the effects of the power surge. The link remained intact during the event.

In summary, the Perry-Ashtabula-Erie West 345-kV line trip at 16:10:38.6 EDT was the point when the Northeast entered a period of transient instability and a loss of generator synchronism.

Figure 5.9. Active and Reactive Power and Voltage from Ontario into Detroit



Western Pennsylvania Separated from New York: 16:10:39 EDT to 16:10:44 EDT

6D) 16:10:39 EDT, Homer City-Watercure Road 345-kV

Homer City-Stolle Road 345-kV: 16:10:39 EDT

6E) South Ripley-Erie East 230-kV, and South Ripley-Dunkirk 230-kV: 16:10:44 EDT

East Towanda-Hillside 230-kV: 16:10:44 EDT

Responding to the surge of power flowing north out of Pennsylvania through New York and Ontario into Michigan, relays on these lines activated on apparent impedance within a five-second period and separated Pennsylvania from New York (Figure 5.10).

At this point, the northern part of the Eastern Interconnection (including eastern Michigan and northern Ohio) remained connected to the rest of the Interconnection at only two locations: (1) in the east through the 500-kV and 230-kV ties between New York and northeast New Jersey, and (2) in the west through the long and therefore fragile 230-kV transmission path connecting Ontario to Manitoba and Minnesota.

Figure 5.10. Western Pennsylvania Separates from New York, 16:10:39 EDT to 16:10:44 EDT

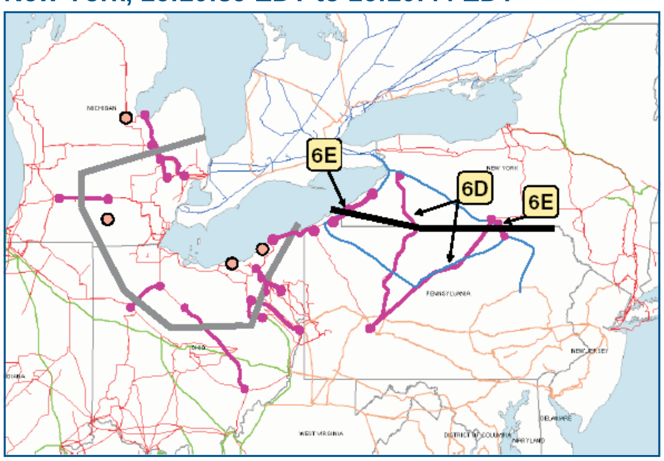
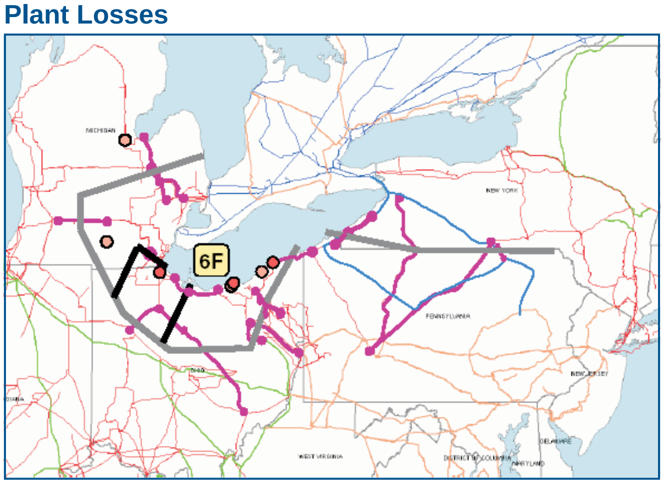


Figure 5.11. More Transmission Line and Power Plant Losses



Because the demand for power in Michigan, Ohio, and Ontario was drawing on lines through New York and Pennsylvania, heavy power flows were moving northward from New Jersey over the New York tie lines to meet those power demands, exacerbating the power swing.

6F) Conditions in Northern Ohio and Eastern Michigan Degraded Further, With More Transmission Lines and Power Plants Failing: 16:10:39 to 16:10:46 EDT

Bayshore-Monroe 345-kV line

Allen Junction-Majestic-Monroe 345-kV line

Majestic 345-kV Substation: one terminal opened on all 345-kV lines

Perry-Ashtabula-Erie West 345-kV line terminal at Ashtabula 345/138-kV substation

Fostoria Central-Galion 345-kV line

Beaver-Davis Besse 345-kV line

Galion-Ohio Central-Muskingum 345 tripped at Galion

Six power plants, for a total of 3,097 MW of generation, tripped off-line:

Lakeshore unit 18 (156 MW, near Cleveland)

Bay Shore Units 1-4 (551 MW near Toledo)

Eastlake 1, 2, and 3 units (403 MW total, near Cleveland)

Avon Lake unit 9 (580 MW, near Cleveland)

Perry 1 nuclear unit (1,223 MW, near Cleveland)

Ashtabula unit 5 (184 MW, near Cleveland)

Back in northern Ohio, the trips of the Majestic 345-kV substation in southeast Michigan, the Bay Shore-Monroe 345-kV line, and the Ashtabula 345/138-kV transformer created a Toledo and Cleveland electrical “island” (Figure 5.11). Frequency in this large island began to fall rapidly. This led to a series of power plants in the area shutting down due to the operation of underfrequency relays, including the Bay Shore units. When the Beaver-Davis Besse 345-kV line connecting Cleveland and Toledo tripped, it left the Cleveland area completely isolated. Cleveland area load was disconnected by automatic underfrequency load-shedding (approximately 1,300

MW in the greater Cleveland area), and another 434 MW of load was interrupted after the generation remaining within this transmission “island” was tripped by under-frequency relays. Portions of Toledo blacked out from automatic under-frequency load-shedding but most of the Toledo load was restored by automatic reclosing of lines such as the East Lima-Fostoria Central 345-kV line and several lines at the Majestic 345-kV substation.

The prolonged period of system-wide low voltage around Detroit caused the remaining generators in that area, then running at maximum mechanical output, to begin to pull out of synchronous operation with the rest of the grid. Those plants raced ahead of system frequency with higher than normal revolutions per second by each generator. But when voltage returned to near-normal, the generator could not fully pull back its rate of revolutions, and ended up producing excessive temporary output levels, still out of step with the system. This is evident in Figure 5.9 (above), which shows at least two sets of generator “pole slips” by plants in the Detroit area between 16:10:40 EDT and 16:10:42 EDT. Several large units around Detroit—Belle River, St. Clair, Greenwood, Monroe and Fermi—all recorded tripping for out-of-step operation due to this cause. The Perry 1 nuclear unit, located on the southern shore of Lake Erie near the border with Pennsylvania, and a number of other units near Cleveland tripped off-line by unit under-frequency protection.

6G) Transmission paths disconnected in New Jersey and northern Ontario, isolating the northeast portion of the Eastern Interconnection: 16:10:42 EDT to 16:10:45 EDT

- Four power plants producing 1,630 MW tripped off-line
  - Greenwood unit 11 and 12 tripped (225 MW near Detroit)
  - Belle River unit 1 tripped (600 MW near Detroit)
  - St. Clair unit 7 tripped (221 MW, DTE unit)
  - Trenton Channel units 7A, 8 and 9 tripped (584 MW, DTE units)
- Keith-Waterman 230-kV tripped, 16:10:43 EDT
- Wawa-Marathon W21-22 230-kV line tripped, 16:10:45 EDT
- Branchburg-Ramapo 500-kV line tripped, 16:10:45 EDT

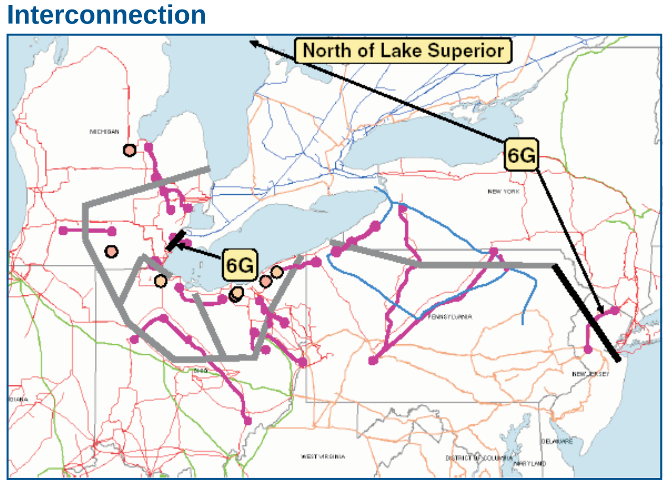
A significant amount of the remaining generation serving Detroit tripped off-line in response to these events. At 16:10:43 EDT, eastern Michigan was still connected to Ontario, but the Keith-Waterman 230-kV line that forms part of that interface disconnected due to apparent impedance (Figure 5.12).

At 16:10:45 EDT, northwest Ontario separated from the rest of Ontario when the Wawa-Marathon 230-kV lines disconnected along the northern shore of Lake Superior. This separation left the loads in the far northwest portion of Ontario connected to the Manitoba and Minnesota systems, and protected them from the blackout.

The Branchburg-Ramapo 500-kV line between New Jersey and New York was the last major transmission path remaining between the Eastern Interconnection and the area ultimately affected by the blackout. That line disconnected at 16:10:45 EDT along with the underlying 230 and 138-kV lines in northeast New Jersey. This left the northeast portion of New Jersey connected to New York, while Pennsylvania and the rest of New Jersey remained connected to the rest of the Eastern Interconnection.

At this point, the Eastern Interconnection was split into two major sections. To the north and east of the separation point lay New York City, northern New Jersey, New York state, New England, the Canadian Maritime provinces, eastern Michigan, the majority of Ontario, and the Québec system. The rest of the Eastern Interconnection, to the south and west of the separation boundary, was not seriously affected by the blackout.

Figure 5.12. Northeast Disconnects from Eastern Interconnection



Phase 7: Several Electrical Islands Formed in Northeast U.S. and Canada: 16:10:46 EDT to 16:12 EDT

Overview of This Phase

New England (except southwestern Connecticut) and the Maritimes separated from New York and remained intact; New York split east to west: 16:10:46 EDT to 16:11:57 EDT. Figure 5.13 illustrates the events of this phase.

During the next 3 seconds, the islanded northern section of the Eastern Interconnection broke apart internally.

7A) New York-New England transmission lines disconnected: 16:10:46 EDT to 16:10:47 EDT

7B) 16:10:49 EDT, New York transmission system split east to west

7C) The Ontario system just west of Niagara Falls and west of St. Lawrence separated from the western New York island: 16:10:50 EDT

7D) Southwest Connecticut separated from New York City: 16:11:22 EDT

7E) Remaining transmission lines between Ontario and eastern Michigan separated: 16:11:57 EDT

Key Phase 7 Events

7A) New York-New England Transmission Lines Disconnected: 16:10:46 EDT to 16:10:49 EDT

Over the period 16:10:46 EDT to 16:10:49 EDT, the New York to New England tie lines tripped. The power swings continuing through the region caused this separation, and caused Vermont to lose approximately 70 MW of load.

The ties between New York and New England disconnected, and most of the New England area along with Canada's Maritime Provinces became an island with generation and demand balanced close enough that it was able to remain operational. New England had been exporting close to 600 MW to New York, and its system experienced continuing fluctuations until it reached electrical equilibrium. Before the Maritimes-New England separated from the Eastern Interconnection at approximately 16:11 EDT, voltages became depressed due to the large power swings across portions of New England. Some large customers disconnected themselves automatically.[2] However, southwestern Connecticut separated from New England and remained tied to the New York system for about 1 minute.

Due to its geography and electrical characteristics, the Quebec system in Canada is tied to the remainder of the Eastern Interconnection via high voltage DC links instead of AC transmission lines. Quebec was able to survive the power surges with only small impacts because the DC connections shielded it from the frequency swings.

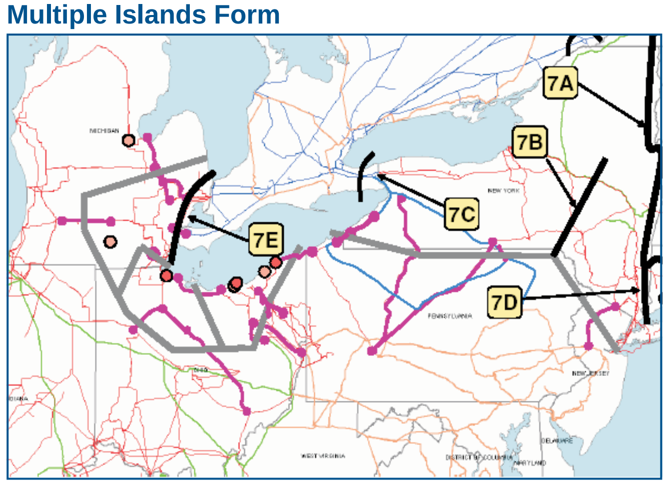
7B) New York Transmission Split East-West: 16:10:49 EDT

The transmission system split internally within New York, with the eastern portion islanding to contain New York City, northern New Jersey and southwestern Connecticut. The western portion of New York remained connected to Ontario and eastern Michigan.

7C) The Ontario System Just West of Niagara Falls and West of St. Lawrence Separated from the Western New York Island: 16:10:50 EDT

At 16:10:50 EDT, Ontario and New York separated west of the Ontario/New York interconnection, due to relay operations which disconnected nine 230-kV lines within Ontario. These left most of Ontario isolated to the north. Ontario's large Beck and Saunders hydro stations, along with some Ontario load, the New York Power Authority's (NYPA) Niagara and St. Lawrence hydro stations, and NYPA's 765-kV AC interconnection with Québec, remained connected to the western New York system, supporting the demand in upstate New York.

Figure 5.13. New York and New England Separate, Multiple Islands Form



From 16:10:49 EDT to 16:10:50 EDT, frequency declined below 59.3 Hz, initiating automatic under-frequency load-shedding in Ontario (2,500 MW), eastern New York and southwestern Connecticut. This load-shedding dropped off about 20% of the load across the eastern New York island and about 10% of Ontario's remaining load. Between 16:10:50 EDT and 16:10:56 EDT, the isolation of the southern Ontario hydro units onto the western New York island, coupled with under-frequency load-shedding in the western New York island, caused the frequency in this island to rise to 63.0 Hz due to excess generation.

Three of the tripped 230-kV transmission circuits near Niagara automatically reconnected Ontario to New York at 16:10:56 EDT by reclosing. Even with these lines reconnected, the main Ontario island (still attached to New York and eastern Michigan) was then extremely deficient in generation, so its frequency declined towards 58.8 Hz, the threshold for the second stage of under-frequency load-shedding. Within the next two seconds another 18% of Ontario demand (4,500 MW) automatically disconnected by under-frequency load-shedding. At 16:11:10 EDT, these same three lines tripped a second time west of Niagara, and New York and most of Ontario separated for a final time. Following this separation, the frequency in Ontario declined to 56 Hz by 16:11:57 EDT. With Ontario still supplying 2,500 MW to the Michigan-Ohio load pocket, the remaining ties with Michigan tripped at 16:11:57 EDT. Ontario system frequency declined, leading to a widespread shutdown at 16:11:58 EDT and loss of 22,500 MW of load in Ontario, including the cities of Toronto, Hamilton and Ottawa.

7D) Southwest Connecticut Separated from New York City: 16:11:22 EDT

In southwest Connecticut, when the Long Mountain-Plum Tree line (connected to the Pleasant Valley substation in New York) disconnected at 16:11:22 EDT, it left about 500 MW of southwest Connecticut demand supplied only through a 138-kV underwater tie to Long Island. About two seconds later, the two 345-kV circuits connecting southeastern New York to Long Island tripped, isolating Long Island and southwest Connecticut, which remained tied together by the underwater Norwalk Harbor to Northport 138-kV cable. The cable tripped about 20 seconds later, causing southwest Connecticut to black out.

Within the western New York island, the 345-kV system remained intact from Niagara east to the Utica area, and from the St. Lawrence/Plattsburgh area south to the Utica area through both the 765-kV and 230-kV circuits. Ontario's Beck and Saunders generation remained connected to New York at Niagara and St. Lawrence, respectively, and this island stabilized with about 50% of the pre-event load remaining. The boundary of this island moved southeastward as a result of the reclosure of Fraser to Coopers Corners 345-kV at 16:11:23 EDT.

As a result of the severe frequency and voltage changes, many large generating units in New York and Ontario tripped off-line. The eastern island of

Under-frequency Load-Shedding

Since in an electrical system load and generation must balance, if a system loses a great deal of generation suddenly it will if necessary drop load to balance that loss. Unless that load drop is managed carefully, such an imbalance can lead to a voltage collapse and widespread outages. In an electrical island with declining frequency, if sufficient load is quickly shed, frequency will begin to rise back toward 60 Hz.

After the blackouts of the 1960s, some utilities installed under-frequency load-shedding mechanisms on their distribution systems. These systems are designed to drop pre-designated customer load automatically if frequency gets too low (since low frequency indicates too little generation relative to load), starting generally when frequency reaches 59.2 Hz. Progressively more load is set to drop as frequency levels fall farther. The last step of customer load shedding is set at the frequency level just above the set point for generation under-frequency protection relays (57.5 Hz), to prevent frequency from falling so low that the generators could be damaged (see Figure 2.4).

Not every utility or control area handles load-shedding in the same way. In NPCC, following the Northeast blackout of 1965, the region adopted automatic load-shedding criteria to prevent a recurrence of the cascade and better protect system equipment from damage due to a high-speed system collapse.

New York, including the heavily populated areas of southeastern New York, New York City, and Long Island, experienced severe frequency and voltage decline. At 16:11:29 EDT, the New Scotland to Leeds 345-kV circuits tripped, separating the island into northern and southern sections. The small remaining load in the northern portion of the eastern island (the Albany area) retained electric service, supplied by local generation until it could be resynchronized with the western New York island.

7E) Remaining Transmission Lines Between Ontario and Eastern Michigan Separated: 16:11:57 EDT

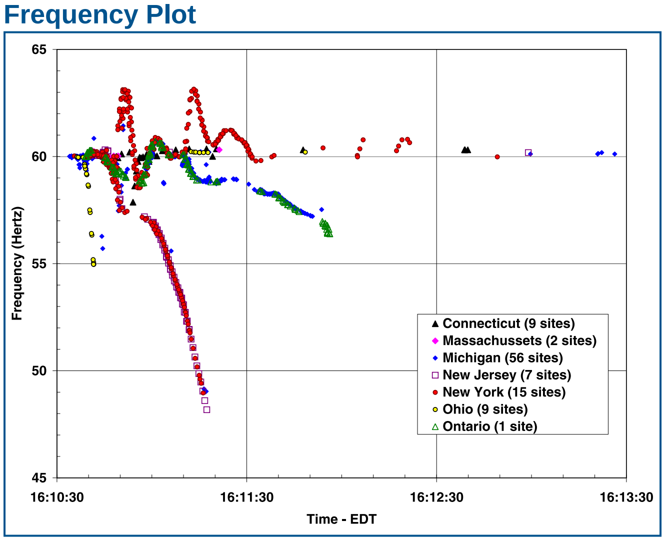
Before the blackout, New England, New York, Ontario, eastern Michigan, and northern Ohio were scheduled net importers of power. When the western and southern lines serving Cleveland, Toledo, and Detroit collapsed, most of the load remained on those systems, but some generation had tripped. This exacerbated the generation/load imbalance in areas that were already importing power. The power to serve this load came through the only major path available, through Ontario (IMO). After most of IMO was separated from New York and generation to the north and east, much of the Ontario load and generation was lost; it took only moments for the transmission paths west from Ontario to Michigan to fail.

When the cascade was over at about 16:12 EDT, much of the disturbed area was completely blacked out, but there were isolated pockets that still had service because load and generation had reached equilibrium. Ontario's large Beck and Saunders hydro stations, along with some Ontario load, the New York Power Authority's (NYPA) Niagara and St. Lawrence hydro stations, and NYPA's 765-kV AC interconnection with Québec, remained connected to the western New York system, supporting demand in upstate New York.

Electrical islanding. Once the northeast became isolated, it grew generation-deficient as more and more power plants tripped off-line to protect themselves from the growing disturbance. The severe swings in frequency and voltage in the area caused numerous lines to trip, so the isolated area broke further into smaller islands. The load/generation mismatch also affected voltages and frequency within these smaller areas, causing further generator trips and automatic under-frequency load-shedding, leading to blackout in most of these areas.

Figure 5.14 shows frequency data collected by the distribution-level monitors of Softswitching Technologies, Inc. (a commercial power quality company serving industrial customers) for the area affected by the blackout. The data reveal at least five separate electrical islands in the Northeast as the cascade progressed. The two paths of red diamonds on the frequency scale reflect the Albany area island (upper path) versus the New York city island, which declined and blacked out much earlier.

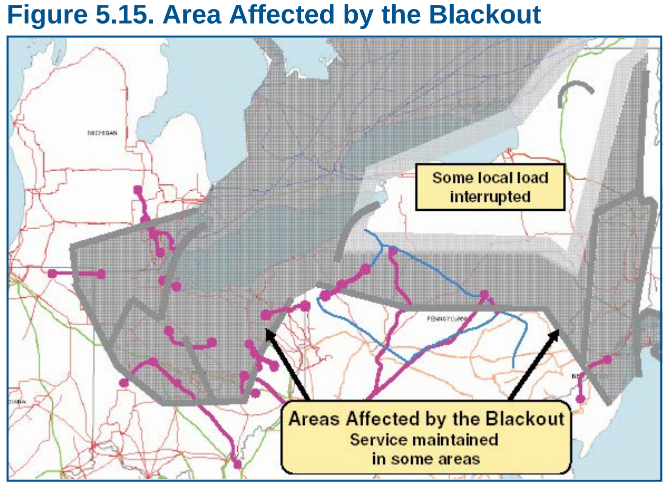
Figure 5.14. Electric Islands Reflected in Frequency Plot



Cascading Sequence Essentially Complete: 16:13 EDT

Most of the Northeast (the area shown in gray in Figure 5.15) was now blacked out. Some isolated areas of generation and load remained on-line for several minutes. Some of those areas in which a close generation-demand balance could be maintained remained operational; other generators ultimately tripped off line and the areas they served were blacked out.

Figure 5.15. Area Affected by the Blackout



One relatively large island remained in operation serving about 5,700 MW of demand, mostly in western New York. Ontario's large Beck and Saunders hydro stations, along with some Ontario load, the New York Power Authority's (NYPA) Niagara and St. Lawrence hydro stations, and NYPA's 765-kV AC interconnection with Québec, remained connected to the western New York system, supporting demand in upstate New York. This island formed the basis for restoration in both New York and Ontario.

The entire cascade sequence is depicted graphically in Figure 5.16 on the following page.

Why the Blackout Stopped Where It Did

Extreme system conditions can damage equipment in several ways, from melting aluminum conductors (excessive currents) to breaking turbine blades on a generator (frequency excursions). The power system is designed to ensure that if conditions on the grid (excessive or inadequate voltage, apparent impedance or frequency) threaten the safe operation of the transmission lines, transformers, or power plants, the threatened equipment automatically separates from the network to protect itself from physical damage. Relays are the devices that effect this protection.

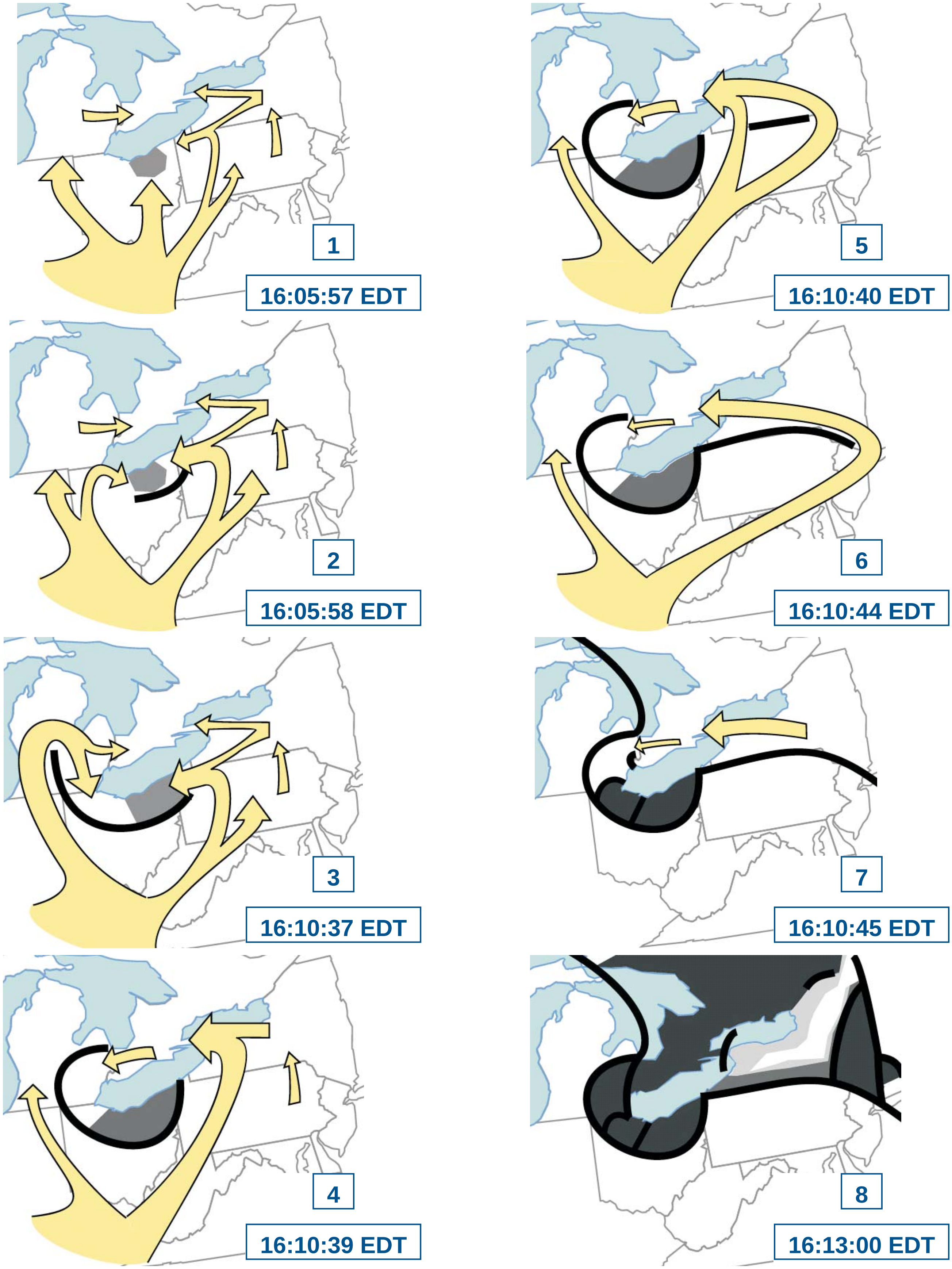
Generators are usually the most expensive units on an electrical system, so system protection schemes are designed to drop a power plant off the system as a self-protective measure if grid conditions become unacceptable. When unstable power swings develop between a group of generators that are losing synchronization (matching frequency) with the rest of the system, the only way to stop the oscillations is to stop the flows entirely by separating all interconnections or ties between the unstable generators and the remainder of the system. The most common way to protect generators from power oscillations is for the transmission system to detect the power swings and trip at the locations detecting the swings—ideally before the swing reaches and harms the generator.

On August 14, the cascade became a race between the power surges and the relays. The lines that tripped first were generally the longer lines, because the relay settings required to protect these lines use a longer apparent impedance tripping zone, which a power swing enters sooner, in comparison to the shorter apparent impedance zone targets set on shorter, networked lines. On August 14, relays on long lines such as the Homer City-Watercure and the Homer City-Stolle Road 345-kV lines in Pennsylvania, that are not highly integrated into the electrical network, tripped quickly and split the grid between the sections that blacked out and those that recovered without further propagating the cascade. This same phenomenon was seen in the Pacific Northwest blackouts of 1996, when long lines tripped before more networked, electrically supported lines.

Transmission line voltage divided by its current flow is called "apparent impedance." Standard transmission line protective relays continuously measure apparent impedance. When apparent impedance drops within the line's protective relay set-points for a given period of time, the relays trip the line. The vast majority of trip operations on lines along the blackout boundaries between PJM and New York (for instance) show high-speed relay targets, which indicate that massive power surges caused each line to trip. To the relays, this massive power surge altered the voltages and currents enough that they appeared to be faults. This power surge was caused by power flowing to those areas that were generation-deficient. These flows occurred purely because of the physics of power flows, with no regard to whether the power flow had been scheduled, because power flows from areas with excess generation into areas that are generation-deficient.

Relative voltage levels across the northeast affected which areas blacked out and which areas stayed on-line. Within the Midwest, there were relatively low reserves of reactive power, so as voltage levels declined many generators in the affected area were operating at maximum reactive power output before the blackout. This left the system little slack to deal with the low voltage conditions by ramping up more generators to higher reactive power output levels, so there was little room to absorb any system "bumps" in voltage or frequency. In contrast, in the northeast—particularly PJM, New York, and ISO-New England—operators were anticipating high power demands on the afternoon of August 14, and had already set up the system to maintain higher voltage levels and therefore had more reactive reserves on-line in anticipation of later afternoon needs. Thus, when the voltage and frequency swings began, these systems had reactive power already or readily available to help buffer their areas against a voltage collapse without widespread generation trips.

Figure 5.16. Cascade Sequence



Legend: Yellow arrows represent the overall pattern of electricity flows. Black lines represent approximate points of separation between areas within the Eastern Interconnect. Gray shading represents areas affected by the blackout.

Voltage Collapse

Although the blackout of August 14 has been labeled as a voltage collapse, it was not a voltage collapse as that term has been traditionally used by power system engineers. Voltage collapse typically occurs on power systems that are heavily loaded, faulted (reducing the number of available paths for power to flow to loads), or have reactive power shortages. The collapse is initiated when reactive power demands of loads can no longer be met by the production and transmission of reactive power. A classic voltage collapse occurs when an electricity system experiences a disturbance that causes a progressive and uncontrollable decline in voltage. Dropping voltage causes a further reduction in reactive power from capacitors and line charging, and still further voltage reductions. If the collapse continues, these voltage reductions cause additional elements to trip, leading to further reduction in voltage and loss of load. At some point the voltage may stabilize but at a much reduced level. In summary, the system begins to fail due to inadequate reactive power supplies rather than due to overloaded facilities.

On August 14, the northern Ohio electricity system did not experience a classic voltage collapse because low voltage never became the primary cause of line and generator tripping. Although voltage was a factor in some of the events that led to the ultimate cascading of the system in Ohio and beyond, the event was not a classic reactive power-driven voltage collapse. Rather, although reactive power requirements were high, voltage levels were within acceptable bounds before individual transmission trips began, and a shortage of reactive power did not trigger the collapse. Voltage levels began to degrade, but not collapse, as early transmission lines were lost due to tree-line contacts causing ground faults. With fewer lines operational, current flowing over the remaining lines increased and voltage decreased (current increases in inverse proportion to the decrease in voltage for a given amount of power flow). Soon, in northern Ohio, lines began to trip out automatically on protection from overloads, rather than from insufficient reactive power. As the cascade spread beyond Ohio, it spread due not to insufficient reactive power, but because of dynamic power swings and the resulting system instability.

On August 14, voltage collapse in some areas was a result, rather than a cause, of the cascade. Significant voltage decay began after the system was already in an N-3 or N-4 contingency situation. Frequency plots over the course of the cascade show areas with too much generation and others with too much load as the system attempted to reach equilibrium between generation and load. As the transmission line failures caused load to drop off, some parts of the system had too much generation, and some units tripped off on over-frequency protection. Frequency fell, more load dropped on under-frequency protection, the remaining generators sped up and then some of them tripped off, and so on. For a period, conditions see-sawed across the northeast, ending with isolated pockets in which generation and load had achieved balance, and wide areas that had blacked out before an equilibrium had been reached.

Why the Generators Tripped Off

At least 263 power plants with more than 531 individual generating units shut down in the August 14 blackout. These U.S. and Canadian plants can be categorized as follows:

By reliability coordination area:

- Hydro Quebec, 5 plants
- Ontario, 92 plants
- ISO-New England, 31 plants
- MISO, 30 plants
- New York ISO, 67 plants
- PJM, 38 plants

By type:

- Conventional steam units, 67 plants (39 coal)
- Combustion turbines, 66 plants (36 combined cycle)
- Nuclear, 10 plants—7 U.S. and 3 Canadian, totaling 19 units (the nuclear unit outages are discussed in Chapter 7)
- Hydro, 101
- Other, 19

There were three categories of generator shutdowns:

1. Excitation system failures during extremely low voltage conditions on portions of the power system
2. Plant control system actions after major disturbances to in-plant thermal/mechanical systems
3. Consequential tripping due to total system disconnection or collapse.

Examples of the three types of separation are discussed below.

Excitation failures. The Eastlake 5 trip at 1:31 p.m. was an excitation system failure—as voltage fell at the generator bus, the generator tried to increase its production of voltage on the coil (excitation) quickly. This caused the generator's excitation protection scheme to trip the plant off to protect its windings and coils from over-heating. Several of the other generators which tripped early in the cascade came off under similar circumstances as excitation systems were overstressed to hold voltages up.

After the cascade was initiated, huge power swings across the torn transmission system and excursions of system frequency put all the units in their path through a sequence of major disturbances that shocked several units into tripping. Plant controls had actuated fast governor action on several of these to turn back the throttle, then turn it forward, only to turn it back again as some frequencies changed several times by as much as 3 Hz (about 100 times normal). Figure 5.17 is a plot of the MW output and frequency for one large unit that nearly survived the disruption but tripped when in-plant hydraulic control pressure limits were eventually violated. After the plant control system called for shutdown, the turbine control valves closed and the generator electrical output ramped down to a preset value before the field excitation tripped and the generator breakers opened to disconnect the unit from the system.

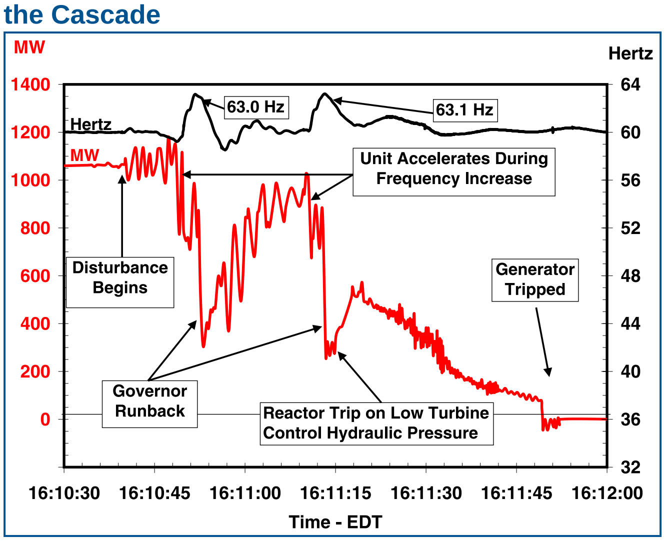
Plant control systems. The second reason for power plant trips was actions or failures of plant control systems. One common cause in this category was a loss of sufficient voltage to in-plant loads. Some plants run their internal cooling and processes (house electrical load) off the generator or off small, in-house auxiliary generators, while others take their power off the main grid. When large power swings or voltage drops reached these plants in the latter category, they tripped off-line because the grid could not supply the plant's in-house power needs reliably.

Consequential trips. Most of the unit separations fell in the third category of consequential tripping—they tripped off-line in response to some outside condition on the grid, not because of any problem internal to the plant. Some generators became completely removed from all loads; because the fundamental operating principle of the grid is that load and generation must balance, if there was no load to be served the power plant shut down in response to over-speed and/or over-voltage protection schemes. Others were overwhelmed because they were among a few power plants within an electrical island, and were suddenly called on to serve huge customer loads, so the imbalance caused them to trip on under-frequency and/or under-voltage protection. A few were tripped by special protection schemes that activated on excessive frequency or loss of pre-studied major transmission elements known to require large blocks of generation rejection.

The maps in Figure 5.18 show the sequence of power plants lost in three blocks of time during the cascade.

The investigation team is still analyzing data on the effect of the cascade on the affected generators, to learn more about how to protect generation and transmission assets and speed system restoration in the future.

Figure 5.17. Events at One Large Generator During the Cascade

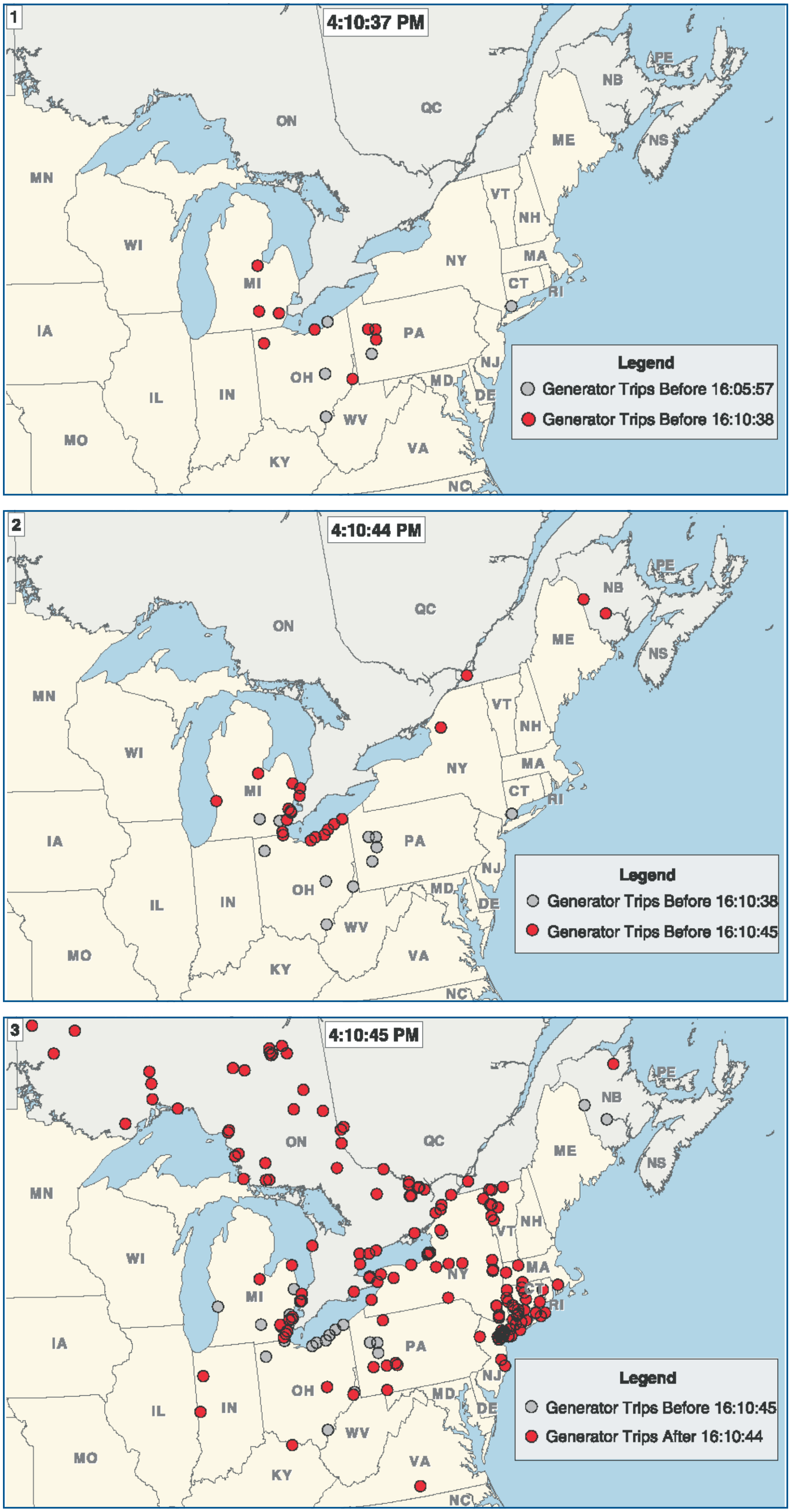


Endnotes

[1] The extensive computer modeling required to determine the expansion and cessation of the blackout (line by line, relay by relay, generator by generator, etc.) has not been performed.

[2] After New England's separation from the Eastern Interconnection occurred, the next several minutes were critical to stabilizing the ISO-NE system. Voltages in New England recovered and over-shot to high due to the combination of load loss, capacitors still in service, lower reactive losses on the transmission system, and loss of generation to regulate system voltage. Over-voltage protective relays operated to trip both transmission and distribution capacitors. Operators in New England brought all fast-start generation on-line by 16:16 EDT. Much of the customer process load was automatically restored. This caused voltages to drop again, putting portions of New England at risk of voltage collapse. Operators manually dropped 80 MW of load in southwest Connecticut by 16:39 EDT, another 325 MW in Connecticut and 100 MW in western Massachusetts by 16:40 EDT. These measures helped to stabilize their island following their separation from the rest of the Eastern Interconnection.

Figure 5.18. Power Plants Tripped During the Cascade



6. The August 14 Blackout Compared With Previous Major North American Outages

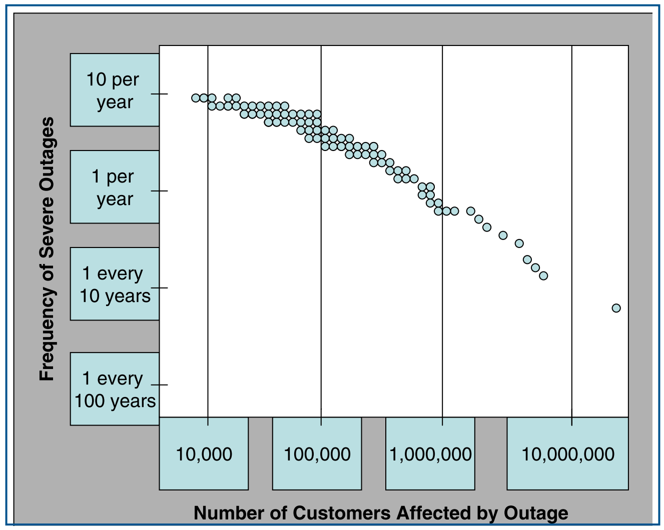
Incidence and Characteristics of Power System Outages

Short, localized outages occur on power systems fairly frequently. System-wide disturbances that affect many customers across a broad geographic area are rare, but they occur more frequently than a normal distribution of probabilities would predict. North American power system outages between 1984 and 1997 are shown in Figure 6.1 by the number of customers affected and the rate of occurrence. While some of these were widespread weather-related events, some were cascading events that, in retrospect, were preventable. Electric power systems are fairly robust and are capable of withstanding one or two contingency events, but they are fragile with respect to multiple contingency events unless the systems are readjusted between contingencies. With the shrinking margin in the current transmission system, it is likely to be more vulnerable to cascading outages than it was in the past, unless effective countermeasures are taken.

As evidenced by the absence of major transmission projects undertaken in North America over the past 10 to 15 years, utilities have found ways to increase the utilization of their existing facilities to meet increasing demands without adding significant high-voltage equipment. Without intervention, this trend is likely to continue. Pushing the system harder will undoubtedly increase reliability challenges. Special protection schemes may be relied on more to deal with particular challenges, but the system still will be less able to withstand unexpected contingencies.

A smaller transmission margin for reliability makes the preservation of system reliability a harder job than it used to be. The system is being operated closer to the edge of reliability than it was just a few years ago. Table 6.1 represents some of the changed conditions that make the preservation of reliability more challenging.

Figure 6.1. North American Power System Outages, 1984-1997



Note: The bubbles represent individual outages in North America between 1984 and 1997.

Source: Adapted from John Doyle, California Institute of Technology, "Complexity and Robustness," 1999. Data from NERC.

If nothing else changed, one could expect an increased frequency of large-scale events as compared to historical experience. The last and most extreme event shown in Figure 6.1 is the August 10, 1996, outage. August 14, 2003, surpassed that event in terms of severity. In addition, two significant outages in the month of September 2003 occurred abroad: one in England and one, initiated in Switzerland, that cascaded over much of Italy.

In the following sections, seven previous outages are reviewed and compared with the blackout of August 14, 2003: (1) Northeast blackout on November 9, 1965; (2) New York City blackout on July 13, 1977; (3) West Coast blackout on December 22, 1982; (4) West Coast blackout on July 2-3, 1996; (5) West Coast blackout on August 10, 1996; (6) Ontario and U.S. North Central blackout on June 25, 1998; and (7) Northeast outages and non-outage disturbances in the summer of 1999.

Outage Descriptions and Major Causal Factors

November 9, 1965: Northeast Blackout

This disturbance resulted in the loss of over 20,000 MW of load and affected 30 million people. Virtually all of New York, Connecticut, Massachusetts, Rhode Island, small segments of northern Pennsylvania and northeastern New Jersey, and substantial areas of Ontario, Canada, were affected. Outages lasted for up to 13 hours. This event resulted in the formation of the North American Electric Reliability Council in 1968.

A backup protective relay operated to open one of five 230-kV lines taking power north from a generating plant in Ontario to the Toronto area. When the flows redistributed instantaneously to the remaining four lines, they tripped out successively in a total of 2.5 seconds. The resultant power swings resulted in a cascading outage that blacked out much of the Northeast.

The major causal factors were as follows:

- Operation of a backup protective relay took a 230-kV line out of service when the loading on the line exceeded the 375-MW relay setting.
- Operating personnel were not aware of the operating set point of this relay.
- Another 230-kV line opened by an overcurrent relay action, and several 115- and 230-kV lines opened by protective relay action.
- Two key 345-kV east-west (Rochester-Syracuse) lines opened due to instability, and several lower voltage lines tripped open.
- Five of 16 generators at the St. Lawrence (Massena) plant tripped automatically in accordance with predetermined operating procedures.
- Following additional line tripouts, 10 generating units at Beck were automatically shut down by low governor oil pressure, and 5 pumping generators were tripped off by overspeed governor control.
- Several other lines then tripped out on under-frequency relay action.

July 13, 1977: New York City Blackout

This disturbance resulted in the loss of 6,000 MW of load and affected 9 million people in New York City. Outages lasted for up to 26 hours. A series of events triggering the separation of the Consolidated Edison system from neighboring systems and its subsequent collapse began when two 345-kV lines on a common tower in Northern Westchester were struck by lightning and tripped out. Over the next hour, despite Consolidated Edison dispatcher actions, the system electrically separated from surrounding systems and collapsed. With the loss of imports, generation in New York City was not sufficient to serve the load in the city.

Major causal factors were:

Table 6.1. Changing Conditions That Affect System Reliability

Previous Conditions	Emerging Conditions
Fewer, relatively large resources	Smaller, more numerous resources
Long-term, firm contracts	Contracts shorter in duration More non-firm transactions, fewer long-term firm transactions
Bulk power transactions relatively stable and predictable	Bulk power transactions relatively variable and less predictable
Assessment of system reliability made from stable base (narrower, more predictable range of potential operating states)	Assessment of system reliability made from variable base (wider, less predictable range of potential operating states)
Limited and knowledgable set of utility players	More players making more transactions, some with less interconnected operation experience; increasing with retail access
Unused transmission capacity and high security margins	High transmission utilization and operation closer to security limits
Limited competition, little incentive for reducing reliability investments	Utilities less willing to make investments in transmission reliability that do not increase revenues
Market rules and reliability rules developed together	Market rules undergoing transition, reliability rules developed separately
Limited wheeling	More system throughput

- Two 345-kV lines connecting Buchanan South to Millwood West were subjected to a phase B to ground fault caused by a lightning strike.
- Circuit breaker operations at the Buchanan South ring bus isolated the Indian Point No. 3 generating unit from any load, and the unit tripped for a rejection of 883 MW of load.
- Loss of the ring bus isolated the 345-kV tie to Ladentown, which had been importing 427 MW, making the cumulative load loss 1,310 MW.
- 18.5 minutes after the first incident, an additional lightning strike caused the loss of two 345-kV lines, which connect Sprain Brook to Buchanan North and Sprain Brook to Millwood West. These two 345-kV lines share common towers between Millwood West and Sprain Brook. One line (Sprain Brook to Millwood West) automatically reclosed and was restored to service in about 2 seconds. The failure of the other line to reclose isolated the last Consolidated Edison interconnection to the Northwest.
- The resulting surge of power from the Northwest caused the loss of the Pleasant Valley to Millwood West line by relay action (a bent contact on one of the relays at Millwood West caused the improper action).
- 23 minutes later, the Leeds to Pleasant Valley 345-kV line sagged into a tree due to overload and tripped out.
- Within a minute, the 345 kV to 138 kV transformer at Pleasant Valley overloaded and tripped off, leaving Consolidated Edison with only three remaining interconnections.
- Within 3 minutes, the Long Island Lighting Co. system operator, on concurrence of the pool dispatcher, manually opened the Jamaica to Valley Stream tie.
- About 7 minutes later, the tap-changing mechanism failed on the Goethals phase-shifter, resulting in the loss of the Linden to Goethals tie to PJM, which was carrying 1,150 MW to Consolidated Edison.
- The two remaining external 138-kV ties to Consolidated Edison tripped on overload, isolating the Consolidated Edison system.
- Insufficient generation in the isolated system caused the Consolidated Edison island to collapse.

December 22, 1982: West Coast Blackout

This disturbance resulted in the loss of 12,350 MW of load and affected over 5 million people in the West. The outage began when high winds caused the failure of a 500-kV transmission tower. The tower fell into a parallel 500-kV line tower, and both lines were lost. The failure of these two lines mechanically cascaded and caused three additional towers to fail on each line. When the line conductors fell they contacted two 230-kV lines crossing under the 500-kV rights-of-way, collapsing the 230-kV lines.

The loss of the 500-kV lines activated a remedial action scheme to control the separation of the interconnection into two pre-engineered islands and trip generation in the Pacific Northwest in order to minimize customer outages and speed restoration. However, delayed operation of the remedial action scheme components occurred for several reasons, and the interconnection separated into four islands.

In addition to the mechanical failure of the transmission lines, analysis of this outage cited problems with coordination of protective schemes, because the generator tripping and separation schemes operated slowly or did not operate as planned. A communication channel component performed sporadically, resulting in delayed transmission of the control signal. The backup separation scheme also failed to operate, because the coordination of relay settings did not anticipate the power flows experienced in this severe disturbance.

In addition, the volume and format in which data were displayed to operators made it difficult to assess the extent of the disturbance and what corrective action should be taken. Time references to events in this disturbance were not tied to a common standard, making real-time evaluation of the situation more difficult.

July 2-3, 1996: West Coast Blackout

This disturbance resulted in the loss of 11,850 MW of load and affected 2 million people in the West. Customers were affected in Arizona, California, Colorado, Idaho, Montana, Nebraska, Nevada, New Mexico, Oregon, South Dakota, Texas, Utah, Washington, and Wyoming in the United States; Alberta and British Columbia in Canada; and Baja California Norte in Mexico. Outages lasted from a few minutes to several hours.

The outage began when a 345-kV transmission line in Idaho sagged into a tree and tripped out. A protective relay on a parallel transmission line also detected the fault and incorrectly tripped a second line. An almost simultaneous loss of these lines greatly reduced the ability of the system to transmit power from the nearby Jim Bridger plant. Other relays tripped two of the four generating units at that plant. With the loss of those two units, frequency in the entire Western Interconnection began to decline, and voltage began to collapse in the Boise, Idaho, area, affecting the California-Oregon AC Intertie transfer limit.

For 23 seconds the system remained in precarious balance, until the Mill Creek to Antelope 230-kV line between Montana and Idaho tripped by zone 3 relay, depressing voltage at Summer Lake Substation and causing the intertie to slip out of synchronism. Remedial action relays separated the system into five pre-engineered islands designed to minimize customer outages and restoration times. Similar conditions and initiating factors were present on July 3; however, as voltage began to collapse in the Boise area, the operator shed load manually and contained the disturbance.

August 10, 1996: West Coast Blackout

This disturbance resulted in the loss of over 28,000 MW of load and affected 7.5 million people in the West. Customers were affected in Arizona, California, Colorado, Idaho, Montana, Nebraska, Nevada, New Mexico, Oregon, South Dakota, Texas, Utah, Washington, and Wyoming in the United States; Alberta and British Columbia in Canada; and Baja California Norte in Mexico. Outages lasted from a few minutes to as long as 9 hours.

Triggered by several major transmission line outages, the loss of generation from McNary Dam, and resulting system oscillations, the Western Interconnection separated into four electrical islands, with significant loss of load and generation. Prior to the disturbance, the transmission system from Canada south through the Northwest into California was heavily loaded with north-to-south power transfers. These flows were due to high Southwest demand caused by hot weather, combined with excellent hydroelectric conditions in Canada and the Northwest.

Very high temperatures in the Northwest caused two lightly loaded transmission lines to sag into untrimmed trees and trip out. A third heavily loaded line also sagged into a tree. Its outage led to the overload and loss of additional transmission lines. General voltage decline in the Northwest and the loss of McNary generation due to incorrectly applied relays caused power oscillations on the California to Oregon AC intertie. The intertie's protective relays tripped these facilities out and caused the Western Interconnection to separate into four islands. Following the loss of the first two lightly loaded lines, operators were unaware that the system was in an insecure state over the next hour, because new operating studies had not been performed to identify needed system adjustment.

June 25, 1998: Ontario and U.S. North Central Blackout

This disturbance resulted in the loss of 950 MW of load and affected 152,000 people in Minnesota, Montana, North Dakota, South Dakota, and Wisconsin in the United States; and Ontario, Manitoba, and Saskatchewan in Canada. Outages lasted up to 19 hours.

A lightning storm in Minnesota initiated a series of events, causing a system disturbance that affected the entire Mid-Continent Area Power Pool (MAPP) Region and the northwestern Ontario Hydro system of the Northeast Power Coordinating Council. A 345-kV line was struck by lightning and tripped out. Underlying lower voltage lines began to overload and trip out, further weakening the system. Soon afterward, lightning struck a second 345-kV line, taking it out of service as well. Following the outage of the second 345-kV line, the remaining lower voltage transmission lines in the area became significantly overloaded, and relays took them out of service. This cascading removal of lines from service continued until the entire northern MAPP Region was separated from the Eastern Interconnection, forming three islands and resulting in the eventual blackout of the northwestern Ontario Hydro system.

Summer of 1999: Northeast U.S. Outages and Non-outage Disturbances

Load in the PJM system on July 6, 1999, was 51,600 MW (approximately 5,000 MW above forecast). PJM used all emergency procedures (including a 5% voltage reduction) except manually tripping load, and imported 5,000 MW from external systems to serve the record customer demand. Load on July 19, 1999, exceeded 50,500 MW. PJM loaded all available eastern PJM generation and again implemented PJM emergency operating procedures from approximately 12 noon into the evening on both days.

During record peak loads, steep voltage declines were experienced on the bulk transmission system. Emergency procedures were implemented to prevent voltage collapse. Low voltage occurred because reactive demand exceeded reactive supply. High reactive demand was due to high electricity demand and high losses resulting from high transfers across the system. Reactive supply was inadequate because generators were unavailable or unable to meet rated reactive capability due to ambient conditions, and because some shunt capacitors were out of service.

Common or Similar Factors Among Major Outages

Among the factors that were either common to the major outages above and the August 14 blackout or had similarities among the events are the following: (1) conductor contact with trees; (2) underestimation of dynamic reactive output of system generators; (3) inability of system operators or coordinators to visualize events on the entire system; (4) failure to ensure that system operation was within safe limits; (5) lack of coordination on system protection; (6) ineffective communication; (7) lack of "safety nets;" and (8) inadequate training of operating personnel. The following sections describe the nature of these factors and list recommendations from previous investigations that are relevant to each.

Conductor Contact With Trees

This factor was an initiating trigger in several of the outages and a contributing factor in the severity of several more. Unlike lightning strikes, for which system operators have fair storm-tracking tools, system operators generally do not have direct knowledge that a line has contacted a tree and faulted. They will sometimes test the line by trying to restore it to service, if that is deemed to be a safe operation. Even if it does go back into service, the line may fault and trip out again as load heats it up. This is most likely to happen when vegetation has not been adequately managed, in combination with hot and windless conditions.

In some of the disturbances, tree contact accounted for the loss of more than one circuit, contributing multiple contingencies to the weakening of the system. Lines usually sag into right-of-way obstructions when the need to retain transmission interconnection is significant. High inductive load composition, such as air conditioning or irrigation pumping, accompanies hot weather and places higher burdens on transmission lines. Losing circuits contributes to voltage decline. Inductive load is unforgiving when voltage declines, drawing additional reactive supply from the system and further contributing to voltage problems.

Recommendations from previous investigations include:

- Paying special attention to the condition of rights-of-way following favorable growing seasons. Very wet and warm spring and summer growing conditions preceded the 1996 outages in the West.
- Careful review of any reduction in operations and maintenance expenses that may contribute to decreased frequency of line patrols or trimming. Maintenance in this area should be strongly directed toward preventive rather than remedial maintenance.

Dynamic Reactive Output of Generators

Reactive supply is an important ingredient in maintaining healthy power system voltages and facilitating power transfers. Inadequate reactive supply was a factor in most of the events. Shunt capacitors and generating resources are the most significant suppliers of reactive power. Operators perform contingency analysis based on how power system elements will perform under various power system conditions. They determine and set transfer limits based on these analyses. Shunt capacitors are easy to model because they are static. Modeling the dynamic reactive output of generators under stressed system conditions has proven to be more challenging. If the model is incorrect, estimating transfer limits will also be incorrect.

In most of the events, the assumed contribution of dynamic reactive output of system generators was greater than the generators actually produced, resulting in more significant voltage problems. Some generators were limited in the amount of reactive power they produced by over-excitation limits, or necessarily derated because of high ambient temperatures. Other generators were controlled to a fixed power factor and did not contribute reactive supply in depressed voltage conditions. Under-voltage load shedding is employed as an automatic remedial action in some interconnections to prevent cascading.

Recommendations from previous investigations concerning voltage support and reactive power management include:

- Communicate changes to generator reactive capability limits in a timely and accurate manner for both planning and operational modeling purposes.
- Investigate the development of a generator MVAr/voltage monitoring process to determine when generators may not be following reported MVAr limits.
- Establish a common standard for generator steady-state and post-contingency (15-minute) MVAr capability definition; determine methodology, testing, and operational reporting requirements.
- Determine the generator service level agreement that defines generator MVAr obligation to help ensure reliable operations.
- Periodically review and field test the reactive limits of generators to ensure that reported MVAr limits are attainable.
- Provide operators with on-line indications of available reactive capability from each generating unit or groups of generators, other VAr sources, and the reactive margin at all critical buses. This information should assist in the operating practice of maximizing the use of shunt capacitors during heavy transfers and thereby increase the availability of system dynamic reactive reserve.
- For voltage instability problems, consider fast automatic capacitor insertion (both series and shunt), direct shunt reactor and load tripping, and under-voltage load shedding.
- Develop and periodically review a reactive margin against which system performance should be evaluated and used to establish maximum transfer levels.

System Visibility Procedures and Operator Tools

Each control area operates as part of a single synchronous interconnection. However, the parties with various geographic or functional responsibilities for reliable operation of the grid do not have visibility of the entire system. Events in neighboring systems may not be visible to an operator or reliability coordinator, or power system data may be available in a control center but not be presented to operators or coordinators as information they can use in making appropriate operating decisions.

Recommendations from previous investigations concerning visibility and tools include:

- Develop communications systems and displays that give operators immediate information on changes in the status of major components in their own and neighboring systems.
- Supply communications systems with uninterruptible power, so that information on system conditions can be transmitted correctly to control centers during system disturbances.
- In the control center, use a dynamic line loading and outage display board to provide operating personnel with rapid and comprehensive information about the facilities available and the operating condition of each facility in service.
- Give control centers the capability to display to system operators computer-generated alternative actions specific to the immediate situation, together with expected results of each action.
- Establish on-line security analysis capability to identify those next and multiple facility outages that would be critical to system reliability from thermal, stability, and post-contingency voltage points of view.
- Establish time-synchronized disturbance monitoring to help evaluate the performance of the interconnected system under stress, and design appropriate controls to protect it.

System Operation Within Safe Limits

Operators in several of the events were unaware of the vulnerability of the system to the next contingency. The reasons were varied: inaccurate modeling for simulation, no visibility of the loss of key transmission elements, no operator monitoring of stability measures (reactive reserve monitor, power transfer angle), and no reassessment of system conditions following the loss of an element and readjustment of safe limits.

Recommendations from previous investigations include:

- Following a contingency, the system must be returned to a reliable state within the allowed readjustment period. Operating guides must be reviewed to ensure that procedures exist to restore system reliability in the allowable time periods.

- Reduce scheduled transfers to a safe and prudent level until studies have been conducted to determine the maximum simultaneous transfer capability limits.
- Reevaluate processes for identifying unusual operating conditions and potential disturbance scenarios, and make sure they are studied before they are encountered in real-time operating conditions.

Coordination of System Protection (Transmission and Generation Elements)

Protective relays are designed to detect abnormal conditions and act locally to isolate faulted power system equipment from the system—both to protect the equipment from damage and to protect the system from faulty equipment. Relay systems are applied with redundancy in primary and backup modes. If one relay fails, another should detect the fault and trip appropriate circuit breakers. Some backup relays have significant "reach," such that non-faulted line overloads or stable swings may be seen as faults and cause the tripping of a line when it is not advantageous to do so. Proper coordination of the many relay devices in an interconnected system is a significant challenge, requiring continual review and revision. Some relays can prevent resynchronizing, making restoration more difficult.

System-wide controls protect the interconnected operation rather than specific pieces of equipment. Examples include controlled islanding to mitigate the severity of an inevitable disturbance and under-voltage or under-frequency load shedding. Failure to operate (or misoperation of) one or more relays as an event developed was a common factor in several of the disturbances.

Recommendations developed after previous outages include:

- Perform system trip tests of relay schemes periodically. At installation the acceptance test should be performed on the complete relay scheme in addition to each individual component so that the adequacy of the scheme is verified.
- Continually update relay protection to fit changing system development and to incorporate improved relay control devices.
- Install sensing devices on critical transmission lines to shed load or generation automatically if the short-term emergency rating is exceeded for a specified period of time. The time delay should be long enough to allow the system operator to attempt to reduce line loadings promptly by other means.
- Review phase-angle restrictions that can prevent reclosing of major interconnections during system emergencies. Consideration should be given to bypassing synchronism-check relays to permit direct closing of critical interconnections when it is necessary to maintain stability of the grid during an emergency.
- Review the need for controlled islanding. Operating guides should address the potential for significant generation/load imbalance within the islands.

Effectiveness of Communications

Under normal conditions, parties with reliability responsibility need to communicate important and prioritized information to each other in a timely way, to help preserve the integrity of the grid. This is especially important in emergencies. During emergencies, operators should be relieved of duties unrelated to preserving the grid. A common factor in several of the events described above was that information about outages occurring in one system was not provided to neighboring systems.

Need for Safety Nets

A safety net is a protective scheme that activates automatically if a pre-specified, significant contingency occurs. When activated, such schemes involve certain costs and inconvenience, but they can prevent some disturbances from getting out of control. These plans involve actions such as shedding load, dropping generation, or islanding, and in all cases the intent is to have a controlled outcome that is less severe than the likely uncontrolled outcome. If a safety net had not been taken out of service in the West in August 1996, it would have lessened the severity of the disturbance from 28,000 MW of load lost to less than 7,200 MW. (It has since been returned to service.) Safety nets should not be relied upon to establish transfer limits, however.

Previous recommendations concerning safety nets include:

- Establish and maintain coordinated programs of automatic load shedding in areas not so equipped, in order to prevent total loss of power in an area that has been separated from the

main network and is deficient in generation. Load shedding should be regarded as an insurance program, however, and should not be used as a substitute for adequate system design.

- Install load-shedding controls to allow fast single-action activation of large-block load shedding by an operator.

Training of Operating Personnel

Operating procedures were necessary but not sufficient to deal with severe power system disturbances in several of the events. Enhanced procedures and training for operating personnel were recommended. Dispatcher training facility scenarios with disturbance simulation were suggested as well. Operators tended to reduce schedules for transactions but were reluctant to call for increased generation—or especially to shed load—in the face of a disturbance that threatened to bring the whole system down.

Previous recommendations concerning training include:

- Thorough programs and schedules for operator training and retraining should be vigorously administered.
- A full-scale simulator should be made available to provide operating personnel with "hands-on" experience in dealing with possible emergency or other system conditions.
- Procedures and training programs for system operators should include anticipation, recognition, and definition of emergency situations.
- Written procedures and training materials should include criteria that system operators can use to recognize signs of system stress and mitigating measures to be taken before conditions degrade into emergencies.
- Line loading relief procedures should not be relied upon when the system is in an insecure state, as these procedures cannot be implemented effectively within the required time frames in many cases. Other readjustments must be used, and the system operator must take responsibility to restore the system immediately.
- Operators' authority and responsibility to take immediate action if they sense the system is starting to degrade should be emphasized and protected.
- The current processes for assessing the potential for voltage instability and the need to enhance the existing operator training programs, operational tools, and annual technical assessments should be reviewed to improve the ability to predict future voltage stability problems prior to their occurrence, and to mitigate the potential for adverse effects on a regional scale.

Comparisons With the August 14 Blackout

The blackout on August 14, 2003, had several causes or contributory factors in common with the earlier outages, including:

- Inadequate vegetation management
- Failure to ensure operation within secure limits
- Failure to identify emergency conditions and communicate that status to neighboring systems
- Inadequate operator training
- Inadequate regional-scale visibility over the power system.

New causal features of the August 14 blackout include: inadequate interregional visibility over the power system; dysfunction of a control area's SCADA/EMS system; and lack of adequate backup capability to that system.

7. Performance of Nuclear Power Plants Affected by the Blackout

Summary

On August 14, 2003, the northeastern United States and Canada experienced a widespread electrical power outage affecting an estimated 50 million people. Nine U.S. nuclear power plants experienced rapid shutdowns (reactor trips) as a consequence of the power outage. Seven nuclear power plants in Canada operating at high power levels at the time of the event also experienced rapid shutdowns. Four other Canadian nuclear plants automatically disconnected from the grid due to the electrical transient but were able to continue operating at a reduced power level and were available to supply power to the grid as it was restored by the transmission system operators. Six nuclear plants in the United States and one in Canada experienced significant electrical disturbances but were able to continue generating electricity. Non-nuclear generating plants in both countries also tripped during the event. Numerous other nuclear plants observed disturbances on the electrical grid but continued to generate electrical power without interruption.

The Nuclear Working Group (NWG) is one of the three Working Groups created to support the U.S.-Canada Power System Outage Task Force. The NWG was charged with identifying all relevant actions by nuclear generating facilities in connection with the outage. Nils Diaz, Chairman of the U.S. Nuclear Regulatory Commission (NRC) and Linda Keen, President and CEO of the Canadian Nuclear Safety Commission (CNSC) are co-chairs of the Working Group, with other members appointed from various State and federal agencies.

During Phase I of the investigation, the NWG focused on collecting and analyzing data from each plant to determine what happened, and whether any activities at the plants caused or contributed to the power outage or involved a significant safety issue. To ensure accuracy, NWG members coordinated their efforts with the Electric System Working Group (ESWG) and the Security Working Group (SWG). NRC and CNSC staff developed a set of technical questions to obtain data from the owners or licensees of the nuclear power plants that would enable their staff to review the response of the nuclear plant systems in detail. The plant data was compared against the plant design to determine if the plant responses were as expected; if they appeared to cause the power outage or contributed to the spread of the outage; and if applicable safety requirements were met.

Having reviewed the operating data for each plant and the response of the nuclear power plants and their staff to the event, the NWG concludes the following:

- All the nuclear plants that shut down or disconnected from the grid responded automatically to grid conditions.
- All the nuclear plants responded in a manner consistent with the plant designs.
- Safety functions were effectively accomplished, and the nuclear plants that tripped were maintained in a safe shutdown condition until their restart.
- The nuclear power plants did not trigger the power system outage or inappropriately contribute to its spread (i.e., to an extent beyond the normal tripping of the plants at expected conditions). Rather, they responded as anticipated in order to protect equipment and systems from the grid disturbances.
- **For nuclear plants in the United States:**
  - Fermi 2, Oyster Creek, and Perry tripped due to main generator trips, which resulted from voltage and frequency fluctuations on the grid. Nine Mile 1 tripped due to a main turbine trip due to frequency fluctuations on the grid.

- FitzPatrick and Nine Mile 2 tripped due to reactor trips, which resulted from turbine control system low pressure due to frequency fluctuations on the grid. Ginna tripped due to a reactor trip which resulted from a large loss of electrical load due to frequency fluctuations on the grid. Indian Point 2 and Indian Point 3 tripped due to a reactor trip on low flow, which resulted when low grid frequency tripped reactor coolant pumps.

- **For nuclear plants in Canada:**
  - At Bruce B and Pickering B, frequency and/or voltage fluctuations on the grid resulted in the automatic disconnection of generators from the grid. For those units that were successful in maintaining the unit generators operational, reactor power was automatically reduced.
  - At Darlington, load swing on the grid led to the automatic reduction in power of the four reactors. The generators were, in turn, automatically disconnected from the grid.
  - Three reactors at Bruce B and one at Darlington were returned to 60% power. These reactors were available to deliver power to the grid on the instructions of the transmission system operator.
  - Three units at Darlington were placed in a zero-power hot state, and four units at Pickering B and one unit at Bruce B were placed in a Guaranteed Shutdown State.

The licensees' return to power operation follows a deliberate process controlled by plant procedures and regulations. Equipment and process problems, whether existing prior to or caused by the event, would normally be addressed prior to restart. The NWG is satisfied that licensees took an appropriately conservative approach to their restart activities, placing a priority on safety.

- **For U.S. nuclear plants:** Ginna, Indian Point 2, Nine Mile 2, and Oyster Creek resumed electrical generation on August 17. FitzPatrick and Nine Mile 1 resumed electrical generation on August 18. Fermi 2 resumed electrical generation on August 20. Perry resumed electrical generation on August 21. Indian Point 3 resumed electrical generation on August 22. Indian Point 3 had equipment issues (failed splices in the control rod drive mechanism power system) that required repair prior to restart. Ginna submitted a special request for enforcement discretion from the NRC to permit mode changes and restart with an inoperable auxiliary feedwater pump. The NRC granted the request for enforcement discretion.

- **For Canadian nuclear plants:** The restart of the Canadian nuclear plants was carried out in accordance with approved Operating Policies and Principles. Three units at Bruce B and one at Darlington were resynchronized with the grid within 6 hours of the event. The remaining three units at Darlington were reconnected by August 17 and 18. Units 5, 6, and 8 at Pickering B and Unit 6 at Bruce B returned to service between August 22 and August 25.

The NWG has found no evidence that the shutdown of the nuclear power plants triggered the outage or inappropriately contributed to its spread (i.e., to an extent beyond the normal tripping of the plants at expected conditions). All the nuclear plants that shut down or disconnected from the grid responded automatically to grid conditions. All the nuclear plants responded in a manner consistent with the plant designs. Safety functions were effectively accomplished, and the nuclear plants that tripped were maintained in a safe shutdown condition until their restart.

Additional details are available in the following sections. Due to the major design differences between nuclear plants in Canada and the United States, the decision was made to have separate sections for each country. This also facilitates the request by the nuclear regulatory agencies in both countries to have sections of the report that stand alone, so that they can also be used as regulatory documents.

Findings of the U.S. Nuclear Working Group

Summary

The U.S. NWG has found no evidence that the shutdown of the nine U.S. nuclear power plants triggered the outage, or inappropriately contributed to its spread (i.e., to an extent beyond the normal tripping of the plants at expected conditions). All nine plants that experienced a reactor trip were responding to grid conditions. The severity of the grid transient caused generators, turbines, or reactor systems at the plants to reach a protective feature limit and actuate a plant shutdown. All nine plants tripped in response to those conditions in a manner consistent with the plant

designs. The nine plants automatically shut down in a safe fashion to protect the plants from the grid transient. Safety functions were effectively accomplished with few problems, and the plants were maintained in a safe shutdown condition until their restart.

The nuclear power plant outages that resulted from the August 14, 2003, power outage were triggered by automatic protection systems for the reactors or turbine-generators, not by any manual operator actions. The NWG has received no information that points to operators deliberately shutting down nuclear units to isolate themselves from instabilities on the grid. In short, only automatic separation of nuclear units occurred.

Regarding the 95 other licensed commercial nuclear power plants in the United States: 4 were already shut down at the time of the power outage, one of which experienced a grid disturbance; 70 operating plants observed some level of grid disturbance but accommodated the disturbances and remained on line, supplying power to the grid; and 21 operating plants did not experience any grid disturbance.

Introduction

In response to the August 14 power outage, the United States and Canada established a joint Power System Outage Task Force. Although many non-nuclear power plants were involved in the power outage, concerns about the nuclear power plants are being specifically addressed by the NWG in supporting of the joint Task Force. The Task Force was tasked with answering two questions:

1. What happened on August 14, 2003, to cause the transmission system to fail resulting in the power outage, and why?
2. Why was the system not able to stop the spread of the outage?

The NRC, which regulates U.S. commercial nuclear power plants, has regulatory requirements for offsite power systems. These requirements address the number of offsite power sources and the ability to withstand certain transients. Offsite power is the normal source of alternating current (AC) power to the safety systems in the plants when the plant main generator is not in operation. The requirements also are designed to protect safety systems from potentially damaging variations (in voltage and frequency) in the supplied power. For loss of offsite power events, the NRC requires emergency generation (typically emergency diesel generators) to provide AC power to safety systems. In addition, the NRC provides oversight of the safety aspects of offsite power issues through its inspection program, by monitoring operating experience, and by performing technical studies.

Phase I: Fact Finding

Phase I of the NWG effort focused on collecting and analyzing data from each plant to determine what happened, and whether any activities at the plants caused or contributed to the power outage or its spread or involved a significant safety issue. To ensure accuracy, a comprehensive coordination effort is ongoing among the working group members and between the NWG, ESWG, and SWG.

The staff developed a set of technical questions to obtain data from the owners or licensees of the nuclear power plants that would enable them to review the response of the nuclear plant systems in detail. Two additional requests for more specific information were made for certain plants. The collection of information from U.S. nuclear power plants was gathered through the NRC regional offices, which had NRC resident inspectors at each plant obtain licensee information to answer the questions. General design information was gathered from plant-specific Updated Final Safety Analysis Reports and other documents.

Plant data were compared against plant designs by the NRC staff to determine whether the plant responses were as expected; whether they appeared to cause the power outage or contributed to the spread of the outage; and whether applicable safety requirements were met. In some cases supplemental questions were developed, and answers were obtained from the licensees to clarify the observed response of the plant. The NWG interfaced with the ESWG to validate some data and to obtain grid information, which contributed to the analysis. The NWG has identified relevant actions by nuclear generating facilities in connection with the power outage.

Typical Design, Operational, and Protective Features of U.S. Nuclear Power Plants

Nuclear power plants have a number of design, operational, and protective features to ensure that

the plants operate safely and reliably. This section describes these features so as to provide a better understanding of how nuclear power plants interact with the grid and, specifically, how nuclear power plants respond to changing grid conditions. While the features described in this section are typical, there are differences in the design and operation of individual plants which are not discussed.

Design Features of Nuclear Power Plants

Nuclear power plants use heat from nuclear reactions to generate steam and use a single steam-driven turbine-generator (also known as the main generator) to produce electricity supplied to the grid.

Connection of the plant switchyard to the grid. The plant switchyard normally forms the interface between the plant main generator and the electrical grid. The plant switchyard has multiple transmission lines connected to the grid system to meet offsite power supply requirements for having reliable offsite power for the nuclear station under all operating and shutdown conditions. Each transmission line connected to the switchyard has dedicated circuit breakers, with fault sensors, to isolate faulted conditions in the switchyard or the connected transmission lines, such as phase-to-phase or phase-to-ground short circuits. The fault sensors are fed into a protection scheme for the plant switchyard that is engineered to localize any faulted conditions with minimum system disturbance.

Connection of the main generator to the switchyard. The plant main generator produces electrical power and transmits that power to the offsite transmission system. Most plants also supply power to the plant auxiliary buses for normal operation of the nuclear generating unit through the unit auxiliary transformer. During normal plant operation, the main generator typically generates electrical power at about 22 kV. The voltage is increased to match the switchyard voltage by the main transformers, and the power flows to the high voltage switchyard through two power circuit breakers.

Power supplies for the plant auxiliary buses. The safety-related and nonsafety auxiliary buses are normally lined up to receive power from the main generator auxiliary transformer, although some plants leave some of their auxiliary buses powered from a startup transformer (that is, from the offsite power distribution system). When plant power generation is interrupted, the power supply automatically transfers to the offsite power source (the startup transformer). If that is not supplying acceptable voltage, the circuit breakers to the safety-related buses open, and the buses are reenergized by the respective fast-starting emergency diesel generators. The nonsafety auxiliary buses will remain deenergized until offsite power is restored.

Operational Features of Nuclear Power Plants

Response of nuclear power plants to changes in switchyard voltage. With the main generator voltage regulator in the automatic mode, the generator will respond to an increase of switchyard voltage by reducing the generator field excitation current. This will result in a decrease of reactive power, normally measured as mega-volts-amperes-reactive (MVAR) from the generator to the switchyard and out to the surrounding grid, helping to control the grid voltage increase. With the main generator voltage regulator in the automatic mode, the generator will respond to a decrease of switchyard voltage by increasing the generator field excitation current. This will result in an increase of reactive power (MVAR) from the generator to the switchyard and out to the surrounding grid, helping to control the grid voltage decrease. If the switchyard voltage goes low enough, the increased generator field current could result in generator field overheating. Over-excitation protective circuitry is generally employed to prevent this from occurring. This protective circuitry may trip the generator to prevent equipment damage.

Under-voltage protection is provided for the nuclear power plant safety buses, and may be provided on nonsafety buses and at individual pieces of equipment. It is also used in some pressurized water reactor designs on reactor coolant pumps (RCPs) as an anticipatory loss of RCP flow signal.

Protective Features of Nuclear Power Plants

The main generator and main turbine have protective features, similar to fossil generating stations, which protect against equipment damage. In general, the reactor protective features are designed to protect the reactor fuel from damage and to protect the reactor coolant system from over-pressure or over-temperature transients. Some trip features also produce a corresponding trip in other components; for example, a turbine trip typically results in a reactor trip above a low power setpoint.

Generator protective features typically include over-current, ground detection, differential relays (which monitor for electrical fault conditions

within a zone of protection defined by the location of the sensors, typically the main generator and all transformers connected directly to the generator output), electrical faults on the transformers connected to the generator, loss of the generator field, and a turbine trip. Turbine protective features typically include over-speed (usually set at 1980 rpm or 66 Hz), low bearing oil pressure, high bearing vibration, degraded condenser vacuum, thrust bearing failure, or generator trip. Reactor protective features typically include trips for over-power, abnormal pressure in the reactor coolant system, low reactor coolant system flow, low level in the steam generators or the reactor vessel, or a trip of the turbine.

Considerations on Returning a U.S. Nuclear Power Plant to Power Production After Switchyard Voltage Is Restored

The following are examples of the types of activities that must be completed before returning a nuclear power plant to power production following a loss of switchyard voltage.

- Switchyard voltage must be normal and stable from an offsite supply. Nuclear power plants are not designed for black-start capability (the ability to start up without external power).
- Plant buses must be energized from the switchyard and the emergency diesel generators restored to standby mode.
- Normal plant equipment, such as reactor coolant pumps and circulating water pumps, must be restarted.
- A reactor trip review report must be completed and approved by plant management, and the cause of the trip must be addressed.
- All plant technical specifications must be satisfied. Technical specifications are issued to each nuclear power plant as part of their license by the NRC. They dictate equipment which must be operable and process parameters which must be met to allow operation of the reactor. Examples of actions that were required following the events of August 14 include refilling the diesel fuel oil storage tanks, refilling the condensate storage tanks, establishing reactor coolant system forced flow, and cooling the suppression pool to normal operating limits. Surveillance tests must be completed as required by technical specifications (for example, operability of the low-range neutron detectors must be demonstrated).
- Systems must be aligned to support the startup.
- Pressures and temperatures for reactor startup must be established in the reactor coolant system for pressurized water reactors.
- A reactor criticality calculation must be performed to predict the control rod withdrawals needed to achieve criticality, where the fission chain reaction becomes self-sustaining due to the increased neutron flux. Certain neutron-absorbing fission products increase in concentration following a reactor trip (followed later by a decrease or decay). At pressurized water reactors, the boron concentration in the primary coolant must be adjusted to match the criticality calculation. Near the end of the fuel cycle, the nuclear power plant may not have enough boron adjustment or control rod worth available for restart until the neutron absorbers have decreased significantly (more than 24 hours after the trip).

It may require about a day or more before a nuclear power plant can restart following a normal trip. Plant trips are a significant transient on plant equipment, and some maintenance may be necessary before the plant can restart. When combined with the infrequent event of loss of offsite power, additional recovery actions will be required. Safety systems, such as emergency diesel generators and safety-related decay heat removal systems, must be restored to normal lineups. These additional actions would extend the time necessary to restart a nuclear plant from this type of event.

Summary of U.S. Nuclear Power Plant Response to and Safety During the August 14 Outage

The NWG's review has not identified any activity or equipment issues at nuclear power plants that caused the transient on August 14, 2003. Nine nuclear power plants tripped within about 60 seconds as a result of the grid disturbance. Additionally, many nuclear power plants experienced a transient due to this grid disturbance.

Nuclear Power Plants That Tripped

The trips at nine nuclear power plants resulted from the plant responses to the grid disturbances. Following the initial grid disturbances, voltages in the plant switchyard fluctuated and reactive

power flows fluctuated. As the voltage regulators on the main generators attempted to compensate, equipment limits were exceeded and protective trips resulted. This happened at Fermi 2 and Oyster Creek. Fermi 2 tripped on a generator field protection trip. Oyster Creek tripped due to a generator trip on high ratio of voltage relative to the electrical frequency.

Also, as the balance between electrical generation and electrical load on the grid was disturbed, the electrical frequency began to fluctuate. In some cases the electrical frequency dropped low enough to actuate protective features. This happened at Indian Point 2, Indian Point 3, and Perry. Perry tripped due to a generator under-frequency trip signal. Indian Point 2 and Indian Point 3 tripped when the grid frequency dropped low enough to trip reactor coolant pumps, which actuated a reactor protective feature.

In other cases, the electrical frequency fluctuated and went higher than normal. Turbine control systems responded in an attempt to control the frequency. Equipment limits were exceeded as a result of the reaction of the turbine control systems to large frequency changes. This led to trips at FitzPatrick, Nine Mile 1, Nine Mile 2, and Ginna. FitzPatrick and Nine Mile 2 tripped on low pressure in the turbine hydraulic control oil system. Nine Mile 1 tripped on turbine light load protection. Ginna tripped due to conditions in the reactor following rapid closure of the turbine control valves in response to high frequency on the grid.

The Perry, Fermi 2, Oyster Creek, and Nine Mile 1 reactors tripped immediately after the generator tripped, although that is not apparent from the times below, because the clocks were not synchronized to the national time standard. The Indian Point 2 and 3, FitzPatrick, Ginna, and Nine Mile 2 reactors tripped before the generators. When the reactor trips first, there is generally a short time delay before the generator output breakers open. The electrical generation decreases rapidly to zero after the reactor trip. Table 7.1 provides the times from the data collected for the reactor trip times, and the time the generator output breakers opened (generator trip), as reported by the ESWG. Additional details on the plants that tripped are given below.

Fermi 2. Fermi 2 is located 25 miles northeast of Toledo, Ohio, in southern Michigan on Lake Erie. It was generating about 1,130 megawatts-electric (MWe) before the event. The reactor tripped due to a turbine trip. The turbine trip was likely the result of multiple generator field protection trips (over-excitation and loss of field) as the Fermi 2 generator responded to a series of rapidly changing transients prior to its loss. This is consistent with data that shows large swings of the Fermi 2 generator MVARs prior to its trip.

Offsite power was subsequently lost to the plant auxiliary buses. The safety buses were deenergized and automatically reenergized from the emergency diesel generators. The operators tripped one emergency diesel generator that was paralled to the grid for testing, after which it automatically loaded. Decay heat removal systems maintained the cooling function for the reactor fuel.

The lowest emergency declaration, an Unusual Event, was declared at about 16:22 EDT due to the loss of offsite power. Offsite power was restored to at least one safety bus at about 01:53 EDT on August 15. The following equipment problems were noted: the Combustion Turbine Generator (the alternate AC power source) failed to start from the control room; however, it was successfully started locally. In addition, the Spent Fuel Pool Cooling System was interrupted for approximately 26 hours and reached a maximum temperature of 130 degrees Fahrenheit (55 degrees Celsius). The main generator was reconnected to the grid at about 01:41 EDT on August 20.

FitzPatrick. FitzPatrick is located about 8 miles northeast of Oswego, NY, in northern New York on Lake Ontario. It was generating about 850 MWe before the event. The reactor tripped due to low pressure in the hydraulic system that controls the turbine control valves. Low pressure in this system typically indicates a large load reject, for

Table 7.1. U.S. Nuclear Plant Trip Times

Nuclear Plant	Reactor Trip[a]	Generator Trip[b]
Perry	16:10:25 EDT	16:10:42 EDT
Fermi 2	16:10:53 EDT	16:10:53 EDT
Oyster Creek . . .	16:10:58 EDT	16:10:57 EDT
Nine Mile 1	16:11 EDT	16:11:04 EDT
Indian Point 2 . .	16:11 EDT	16:11:09 EDT
Indian Point 3 . .	16:11 EDT	16:11:23 EDT
FitzPatrick	16:11:04 EDT	16:11:32 EDT
Ginna.	16:11:36 EDT	16:12:17 EDT
Nine Mile 2	16:11:48 EDT	16:11:52 EDT

[a]As determined from licensee data (which may not be synchronized to the national time standard).

[b]As reported by the Electrical System Working Group (synchronized to the national time standard).

which a reactor trip is expected. In this case the pressure in the system was low because the control system was rapidly manipulating the turbine control valves to control turbine speed, which was being affected by grid frequency fluctuations.

Immediately preceding the trip, both significant over-voltage and under-voltage grid conditions were experienced. Offsite power was subsequently lost to the plant auxiliary buses. The safety buses were deenergized and automatically reenergized from the emergency diesel generators.

The lowest emergency declaration, an Unusual Event, was declared at about 16:26 EDT due to the loss of offsite power. Decay heat removal systems maintained the cooling function for the reactor fuel. Offsite power was restored to at least one safety bus at about 23:07 EDT on August 14. The main generator was reconnected to the grid at about 06:10 EDT on August 18.

Ginna. Ginna is located 20 miles northeast of Rochester, NY, in northern New York on Lake Ontario. It was generating about 487 MWe before the event. The reactor tripped due to Over-Temperature-Delta-Temperature. This trip signal protects the reactor core from exceeding temperature limits. The turbine control valves closed down in response to the changing grid conditions. This caused a temperature and pressure transient in the reactor, resulting in an Over-Temperature-Delta-Temperature trip.

Offsite power was not lost to the plant auxiliary buses. In the operators' judgement, offsite power was not stable, so they conservatively energized the safety buses from the emergency diesel generators. Decay heat removal systems maintained the cooling function for the reactor fuel. Offsite power was not lost, and stabilized about 50 minutes after the reactor trip.

The lowest emergency declaration, an Unusual Event, was declared at about 16:46 EDT due to the degraded offsite power. Offsite power was restored to at least one safety bus at about 21:08 EDT on August 14. The following equipment problems were noted: the digital feedwater control system behaved in an unexpected manner following the trip, resulting in high steam generator levels; there was a loss of RCP seal flow indication, which complicated restarting the pumps; and at least one of the power-operated relief valves experienced minor leakage following proper operation and closure during the transient. Also, one of the motor-driven auxiliary feedwater pumps was damaged after running with low flow conditions due to an improper valve alignment. The redundant pumps supplied the required water flow.

The NRC issued a Notice of Enforcement Discretion to allow Ginna to perform mode changes and restart the reactor with one auxiliary feedwater (AFW) pump inoperable. Ginna has two AFW pumps, one turbine-driven AFW pump, and two standby AFW pumps, all powered from safety-related buses. The main generator was reconnected to the grid at about 20:38 EDT on August 17.

Indian Point 2. Indian Point 2 is located 24 miles north of New York City on the Hudson River. It was generating about 990 MWe before the event. The reactor tripped due to loss of a reactor coolant pump that tripped because the auxiliary bus frequency fluctuations actuated the under-frequency relay, which protects against inadequate coolant flow through the reactor core. This reactor protection signal tripped the reactor, which resulted in turbine and generator trips.

The auxiliary bus experienced the under-frequency due to fluctuating grid conditions. Offsite power was lost to all the plant auxiliary buses. The safety buses were reenergized from the emergency diesel generators. Decay heat removal systems maintained the cooling function for the reactor fuel.

The lowest emergency declaration, an Unusual Event, was declared at about 16:25 EDT due to the loss of offsite power for more than 15 minutes. Offsite power was restored to at least one safety bus at about 20:02 EDT on August 14. The following equipment problems were noted: the service water to one of the emergency diesel generators developed a leak; a steam generator atmospheric dump valve did not control steam generator pressure in automatic and had to be shifted to manual; a steam trap associated with the turbine-driven AFW pump failed open, resulting in operators securing the turbine after 2.5 hours; loss of instrument air required operators to take manual control of charging and a letdown isolation occurred; and operators in the field could not use radios. The main generator was reconnected to the grid at about 12:58 EDT on August 17.

Indian Point 3. Indian Point 3 is located 24 miles north of New York City on the Hudson River. It was generating about 1,010 MWe before the event. The reactor tripped due to loss of a reactor coolant pump that tripped because the auxiliary bus

frequency fluctuations actuated the under-frequency relay, which protects against inadequate coolant flow through the reactor core. This reactor protection signal tripped the reactor, which resulted in turbine and generator trips.

The auxiliary bus experienced the under-frequency due to fluctuating grid conditions. Offsite power was lost to all the plant auxiliary buses. The safety buses were reenergized from the emergency diesel generators. Decay heat removal systems maintained the cooling function for the reactor fuel.

The lowest emergency declaration, an Unusual Event, was declared at about 16:23 EDT due to the loss of offsite power for more than 15 minutes. Offsite power was restored to at least one safety bus at about 20:12 EDT on August 14. The following equipment problems were noted: a steam generator safety valve lifted below its desired setpoint and was gagged; loss of instrument air, including failure of the diesel backup compressor to start and failure of the backup nitrogen system, resulted in manual control of atmospheric dump valves and AFW pumps needing to be secured to prevent overfeeding the steam generators; a blown fuse in a battery charger resulted in a longer battery discharge; a control rod drive mechanism cable splice failed, and there were high resistance readings on 345-kV breaker-1. These equipment problems required correction prior to start-up, which delayed the startup. The main generator was reconnected to the grid at about 05:03 EDT on August 22.

Nine Mile 1. Nine Mile 1 is located 6 miles northeast of Oswego, NY, in northern New York on Lake Ontario. It was generating about 600 MWe before the event. The reactor tripped in response to a turbine trip. The turbine tripped on light load protection (which protects the turbine against a loss of electrical load), when responding to fluctuating grid conditions. The turbine trip caused fast closure of the turbine valves, which, through acceleration relays on the control valves, create a signal to trip the reactor. After a time delay of 10 seconds, the generator tripped on reverse power.

The safety buses were automatically deenergized due to low voltage and automatically reenergized from the emergency diesel generators. Decay heat removal systems maintained the cooling function for the reactor fuel.

The lowest emergency declaration, an Unusual Event, was declared at about 16:33 EDT due to the degraded offsite power. Offsite power was restored to at least one safety bus at about 23:39 EDT on August 14. The following additional equipment problems were noted: a feedwater block valve failed "as is" on the loss of voltage, resulting in a high reactor vessel level; fuses blew in fire circuits, causing control room ventilation isolation and fire panel alarms; and operators were delayed in placing shutdown cooling in service for several hours due to lack of procedure guidance to address particular plant conditions encountered during the shutdown. The main generator was reconnected to the grid at about 02:08 EDT on August 18.

Nine Mile 2. Nine Mile 2 is located 6 miles northeast of Oswego, NY, in northern New York on Lake Ontario. It was generating about 1,193 MWe before the event. The reactor scrammed due to the actuation of pressure switches which detected low pressure in the hydraulic system that controls the turbine control valves. Low pressure in this system typically indicates a large load reject, for which a reactor trip is expected. In this case the pressure in the system was low because the control system was rapidly manipulating the turbine control valves to control turbine speed, which was being affected by grid frequency fluctuations.

After the reactor tripped, several reactor level control valves did not reposition, and with the main feedwater system continuing to operate, a high water level in the reactor caused a turbine trip, which caused a generator trip. Offsite power was degraded but available to the plant auxiliary buses. The offsite power dropped below the normal voltage levels, which resulted in the safety buses being automatically energized from the emergency diesel generators. Decay heat removal systems maintained the cooling function for the reactor fuel.

The lowest emergency declaration, an Unusual Event, was declared at about 17:00 EDT due to the loss of offsite power to the safety buses for more than 15 minutes. Offsite power was restored to at least one safety bus at about 01:33 EDT on August 15. The following additional equipment problem was noted: a tap changer on one of the offsite power transformers failed, complicating the restoration of one division of offsite power. The main generator was reconnected to the grid at about 19:34 EDT on August 17.

Oyster Creek. Oyster Creek is located 9 miles south of Toms River, NJ, near the Atlantic Ocean. It was generating about 629 MWe before the event.

The reactor tripped due to a turbine trip. The turbine trip was the result of a generator trip due to actuation of a high Volts/Hz protective trip. The Volts/Hz trip is a generator/transformer protective feature. The plant safety and auxiliary buses transferred from the main generator supply to the offsite power supply following the plant trip. Other than the plant transient, no equipment or performance problems were determined to be directly related to the grid problems.

Post-trip the operators did not get the mode switch to shutdown before main steam header pressure reached its isolation setpoint. The resulting MSIV closure complicated the operator's response because the normal steam path to the main condenser was lost. The operators used the isolation condensers for decay heat removal. The plant safety and auxiliary buses remained energized from offsite power for the duration of the event, and the emergency diesel generators were not started. Decay heat removal systems maintained the cooling function for the reactor fuel. The main generator was reconnected to the grid at about 05:02 EDT on August 17.

Perry. Perry is located 7 miles northeast of Painesville, OH, in northern Ohio on Lake Erie. It was generating about 1,275 MWe before the event. The reactor tripped due to a turbine control valve fast closure trip signal. The turbine control valve fast closure trip signal was due to a generator underfrequency trip signal that tripped the generator and the turbine and was triggered by grid frequency fluctuations. Plant operators noted voltage fluctuations and spikes on the main transformer, and the Generator Out-of-Step Supervisory relay actuated approximately 30 minutes before the trip. This supervisory relay senses a ground fault on the grid. The purpose is to prevent a remote fault on the grid from causing a generator out-of-step relay to activate, which would result in a generator trip. Approximately 30 seconds prior to the trip operators noted a number of spikes on the generator field volt meter, which subsequently went offscale high. The MVAR and MW meters likewise went offscale high.

The safety buses were deenergized and automatically reenergized from the emergency diesel generators. Decay heat removal systems maintained the cooling function for the reactor fuel. The following equipment problems were noted: a steam bypass valve opened; a reactor water clean-up system pump tripped; the off-gas system isolated, and a keep-fill pump was found to be air-bound, requiring venting and filling before the residual heat removal system loop A and the low pressure core spray system could be restored to service.

The lowest emergency declaration, an Unusual Event, was declared at about 16:20 EDT due to the loss of offsite power. Offsite power was restored to at least one safety bus at about 18:13 EDT on August 14. The main generator was reconnected to the grid at about 23:15 EDT on August 21. After the plant restarted, a surveillance test indicated a problem with one emergency diesel generator. An NRC special inspection is in progress, reviewing emergency diesel generator performance and the keep-fill system.

Nuclear Power Plants With a Significant Transient

The electrical disturbance on August 14 had a significant impact on seven plants that continued to remain connected to the grid. For this review, significant impact means that these plants had significant load adjustments that resulted in bypassing steam from the turbine generator, opening of relief valves, or requiring the onsite emergency diesel generators to automatically start due to low voltage.

Nuclear Power Plants With a Non-Significant Transient

Sixty-four nuclear power plants experienced non-significant transients caused by minor disturbances on the electrical grid. These plants were able to respond to the disturbances through normal control systems. Examples of these transients included changes in load of a few megawatts or changes in frequency of a few-tenths Hz.

Nuclear Power Plants With No Transient

Twenty-four nuclear power plants experienced no transient and saw essentially no disturbances on the grid, or were shut down at the time of the transient.

General Observations Based on the Facts Found During Phase One

The NWG has found no evidence that the shutdown of U.S. nuclear power plants triggered the outage or inappropriately contributed to its spread (i.e., to an extent beyond the normal tripping of the plants at expected conditions). This review did not identify any activity or equipment issues that appeared to start the transient on August 14, 2003. All nine plants that experienced a reactor trip were responding to grid conditions. The severity

of the transient caused generators, turbines, or reactor systems to reach a protective feature limit and actuate a plant shutdown.

All nine plants tripped in response to those conditions in a manner consistent with the plant designs. All nine plants safely shut down. All safety functions were effectively accomplished, with few problems, and the plants were maintained in a safe shutdown condition until their restart. Fermi 2, Nine Mile 1, Oyster Creek, and Perry tripped on turbine and generator protective features. FitzPatrick, Ginna, Indian Point 2 and 3, and Nine Mile 2 tripped on reactor protective features.

Nine plants used their emergency diesel generators to power their safety-related buses during the power outage. Offsite power was restored to the safety buses after the grid was energized and the plant operators, in consultation with the transmission system operators, decided the grid was stable. Although the Oyster Creek plant tripped, offsite power was never lost to their safety buses and the emergency diesel generators did not start and were not required. Another plant, Davis-Besse, was already shut down but lost power to the safety buses. The emergency diesel generators started and provided power to the safety buses as designed.

For the eight remaining tripped plants and Davis-Besse (which was already shut down prior to the events of August 14), offsite power was restored to at least one safety bus after a period of time ranging from about 2 hours to about 14 hours, with an average time of about 7 hours. Although Ginna did not lose offsite power, the operators judged offsite power to be unstable and realigned the safety buses to the emergency diesel generators. The second phase of the Power System Outage Task Force will consider the implications of this in developing recommendations for future improvements.

The licensees' return to power operation follows a deliberate process controlled by plant procedures and NRC regulations. Ginna, Indian Point 2, Nine Mile 2, and Oyster Creek resumed electrical generation on August 17. FitzPatrick and Nine Mile 1 resumed electrical generation on August 18. Fermi 2 resumed electrical generation on August 20. Perry resumed electrical generation on August 21. Indian Point 3 resumed electrical generation on August 22. Indian Point 3 had equipment issues (failed splices in the control rod drive mechanism power system) that required repair prior to restart. Ginna submitted a special request for enforcement discretion from the NRC to permit mode changes and restart with an inoperable auxiliary feedwater pump. The NRC granted the request for enforcement discretion.

Findings of the Canadian Nuclear Working Group

Summary

On the afternoon of August 14, 2003, southern Ontario, along with the northeastern United States, experienced a widespread electrical power system outage. Eleven nuclear power plants in Ontario operating at high power levels at the time of the event either automatically shut down as a result of the grid disturbance or automatically reduced power while waiting for the grid to be reestablished. In addition, the Point Lepreau Nuclear Generating Station in New Brunswick was forced to reduce electricity production for a short period.

The Canadian NWG was mandated to: review the sequence of events for each Canadian nuclear plant; determine whether any events caused or contributed to the power system outage; evaluate any potential safety issues arising as a result of the event; evaluate the effect on safety and the reliability of the grid of design features, operating procedures, and regulatory requirements at Canadian nuclear power plants; and assess the impact of associated regulator performance and regulatory decisions.

In Ontario, 11 nuclear units were operating and delivering power to the grid at the time of the grid disturbance: 4 at Bruce B, 4 at Darlington, and 3 at Pickering B. Of the 11 reactors, 7 shut down as a result of the event (1 at Bruce B, 3 at Darlington, and 3 at Pickering B). Four reactors (3 at Bruce B and 1 at Darlington) disconnected safely from the grid but were able to avoid shutting down and were available to supply power to the Ontario grid as soon as reconnection was enabled by Ontario's Independent Market Operator (IMO).

New Brunswick Power's Point Lepreau Generating Station responded to the loss of grid event by cutting power to 460 MW, returning to fully stable conditions at 16:35 EDT, within 25 minutes of the event. Hydro Québec's (HQ) grid was not affected by the power system outage, and HQ's Gentilly-2 nuclear station continued to operate normally.

Having reviewed the operating data for each plant and the responses of the power stations and their staff to the event, the Canadian NWG concludes the following:

- None of the reactor operators had any advanced warning of impending collapse of the grid.
  - Trend data obtained indicate stable conditions until a few minutes before the event.
  - There were no prior warnings from Ontario's IMO.
- Canadian nuclear power plants did not trigger the power system outage or contribute to its spread. Rather they responded, as anticipated, in order to protect equipment and systems from the grid disturbances. Plant data confirm the following.
  - At Bruce B and Pickering B, frequency and/or voltage fluctuations on the grid resulted in the automatic disconnection of generators from the grid. For those units that were successful in maintaining the unit generators operational, reactor power was automatically reduced.
  - At Darlington, load swing on the grid led to the automatic reduction in power of the four reactors. The generators were, in turn, automatically disconnected from the grid.
  - Three reactors at Bruce B and one at Darlington were returned to 60% power. These ractors were available to deliver power to the grid on the instructions of the IMO.
  - Three units at Darlington were placed in a zero-power hot state, and four units at Pickering B and one unit at Bruce B were placed in a guaranteed shutdown state.
- There were no risks to health and safety of workers or the public as a result of the shutdown of the reactors.
  - Turbine, generator, and reactor automatic safety systems worked as designed to respond to the loss of grid.
  - Station operating staff and management followed approved Operating Policies & Principles (OP&Ps) in responding to the loss of grid. At all times, operators and shift supervisors made appropriately conservative decisions in favor of protecting health and safety.

The Canadian NWG commends the staff of Ontario Power Generation and Bruce Power for their response to the power system outage. At all times, staff acted in accordance with established OP&Ps, and took an appropriately conservative approach to decisions.

During the course of its review, the NWG also identified the following secondary issues:

- Equipment problems and design limitations at Pickering B resulted in a temporary reduction in the effectiveness of some of the multiple safety barriers, although the equipment failure was within the unavailability targets found in the OP&Ps approved by the CNSC as part of Ontario Power Generation's licence.
- Existing OP&Ps place constraints on the use of adjuster rods to respond to events involving rapid reductions in reactor power. While greater flexibility with respect to use of adjuster rods would not have prevented the shutdown, some units, particularly those at Darlington, might have been able to return to service less than 1 hour after the initiating event.
- Off-site power was unavailable for varying periods of time, from approximately 3 hours at Bruce B to approximately 9 hours at Pickering A. Despite the high priority assigned by the IMO to restoring power to the nuclear stations, the stations had some difficulty in obtaining timely information about the status of grid recovery and the restoration of Class IV power. This information is important for Ontario Power Generation's and Bruce Power's response strategy.
- Required regulatory approvals from CNSC staff were obtained quickly and did not delay the restart of the units; however, CNSC staff was unable to immediately activate the CNSC's Emergency Operation Centre because of loss of power to the CNSC's head office building. CNSC staff, therefore, established communications with licensees and the U.S. NRC from other locations.

Introduction

The primary focus of the Canadian NWG during Phase I was to address nuclear power plant response relevant to the power outage of August 14, 2003. Data were collected from each power plant and analyzed in order to determine: the cause of the power outage; whether any activities at these plants caused or contributed to the power outage; and whether there were any significant safety issues. In order to obtain reliable and comparable information and data from each nuclear

power plant, a questionnaire was developed to help pinpoint how each nuclear power plant responded to the August 14 grid transients. Where appropriate, additional information was obtained from the ESWG and SWG.

The operating data from each plant were compared against the plant design specifications to determine whether the plants responded as expected. Based on initial plant responses to the questionnaire, supplemental questions were developed, as required, to further clarify outstanding matters. Supplementary information on the design features of Ontario's nuclear power plants was also provided by Ontario Power Generation and Bruce Power. The Canadian NWG also consulted a number of subject area specialists, including CNSC staff, to validate the responses to the questionnaire and to ensure consistency in their interpretation.

Typical Design, Operational, and Protective Features of CANDU Nuclear Power Plants

There are 22 CANDU nuclear power reactors in Canada—20 located in Ontario at 5 multi-unit stations (Pickering A and Pickering B located in Pickering, Darlington located in the Municipality of Clarington, and Bruce A and Bruce B located near Kincardine). There are also single-unit CANDU stations at Bécancour, Québec (Gentilly-2), and Point Lepreau, New Brunswick.

In contrast to the pressurized water reactors used in the United States, which use enriched uranium fuel and a light water coolant-moderator, all housed in a single, large pressure vessel, a CANDU reactor uses fuel fabricated from natural uranium, with heavy water as the coolant and moderator. The fuel and pressurized heavy water coolant are contained in 380 to 480 pressure tubes housed in a calandria containing the heavy water moderator under low pressure. Heat generated by the fuel is removed by heavy water coolant that flows through the pressure tubes and is then circulated to the boilers to produce steam from demineralized water.

While the use of natural uranium fuel offers important benefits from the perspectives of safeguards and operating economics, one drawback is that it restricts the ability of a CANDU reactor to recover from a large power reduction. In particular, the lower reactivity of natural uranium fuel means that CANDU reactors are designed with a small number of control rods (called "adjuster rods") that are only capable of accommodating power reductions to 60%. The consequence of a larger power reduction is that the reactor will "poison out" and cannot be made critical for up to 2 days following a power reduction. By comparison, the use of enriched fuel enables a typical pressurized water reactor to operate with a large number of control rods that can be withdrawn to accommodate power reductions to zero power.

A unique feature of some CANDU plants—namely, Bruce B and Darlington—is a capability to maintain the reactor at 60% full power if the generator becomes disconnected from the grid and to maintain this "readiness" condition if necessary for days. Once reconnected to the grid, the unit can be loaded to 60% full power within several minutes and can achieve full power within 24 hours.

As with other nuclear reactors, CANDU reactors normally operate continuously at full power except when shut down for maintenance and inspections. As such, while they provide a stable source of baseload power generation, they cannot provide significant additional power in response to sudden increases in demand. CANDU power plants are not designed for black-start operation; that is, they are not designed to start up in the absence of power from the grid.

Electrical Distribution Systems

The electrical distribution systems at nuclear power plants are designed to satisfy the high safety and reliability requirements for nuclear systems. This is achieved through flexible bus arrangements, high capacity standby power generation, and ample redundancy in equipment.

Where continuous power is required, power is supplied either from batteries (for continuous DC power, Class I) or via inverters (for continuous AC power, Class II). AC supply for safety-related equipment, which can withstand short interruption (on the order of 5 minutes), is provided by Class III power. Class III power is nominally supplied through Class IV; when Class IV becomes unavailable, standby generators are started automatically, and the safety-related loads are picked up within 5 minutes of the loss of Class IV power.

The Class IV power is an AC supply to reactor equipment and systems that can withstand longer interruptions in power. Class IV power can be supplied either from the generator through a

transformer or from the grid by another transformer. Class IV power is not required for reactors to shut down safely.

In addition to the four classes of power described above, there is an additional source of power known as the Emergency Power System (EPS). EPS is a separate power system consisting of its own on-site power generation and AC and DC distribution systems whose normal supply is from the Class III power system. The purpose of the EPS system is to provide power to selected safety-related loads following common mode incidents, such as seismic events.

Protective Features of CANDU Nuclear Power Plants

CANDU reactors typically have two separate, independent and diverse systems to shut down the reactor in the event of an accident or transients in the grid. Shutdown System 1 (SDS1) consists of a large number of cadmium rods that drop into the core to decrease the power level by absorbing neutrons. Shutdown System 2 (SDS2) consists of high-pressure injection of gadolinium nitrate into the low-pressure moderator to decrease the power level by absorbing neutrons. Although Pickering A does not have a fully independent SDS2, it does have a second shutdown mechanism, namely, the fast drain of the moderator out of the calandria; removal of the moderator significantly reduces the rate of nuclear fission, which reduces reactor power. Also, additional trip circuits and shutoff rods have recently been added to Pickering A Unit 4 (Shutdown System Enhancement, or SDS-E). Both SDS1 and SDS2 are capable of reducing reactor power from 100% to about 2% within a few seconds of trip initiation.

Fuel Heat Removal Features of CANDU Nuclear Power Plants

Following the loss of Class IV power and shutdown of the reactor through action of SDS1 and/or SDS2, significant heat will continue to be generated in the reactor fuel from the decay of fission products. The CANDU design philosophy is to provide defense in depth in the heat removal systems.

Immediately following the trip and prior to restoration of Class III power, heat will be removed from the reactor core by natural circulation of coolant through the Heat Transport System main circuit following rundown of the main Heat Transport pumps (first by thermosyphoning and later by intermittent buoyancy induced flow). Heat will be rejected from the secondary side of the steam generators through the atmospheric steam discharge valves. This mode of operation can be sustained for many days with additional feedwater supplied to the steam generators via the Class III powered auxiliary steam generator feed pump(s).

In the event that the auxiliary feedwater system becomes unavailable, there are two alternate EPS powered water supplies to steam generators, namely, the Steam Generator Emergency Coolant System and the Emergency Service Water System. Finally, a separate and independent means of cooling the fuel is by forced circulation by means of the Class III powered shutdown cooling system; heat removal to the shutdown cooling heat exchangers is by means of the Class III powered components of the Service Water System.

CANDU Reactor Response to Loss-of-Grid Event

Response to Loss of Grid

In the event of disconnection from the grid, power to safely shut down the reactor and maintain essential systems will be supplied from batteries and standby generators. The specific response of a reactor to disconnection from the grid will depend on the reactor design and the condition of the unit at the time of the event.

60% Reactor Power: All CANDU reactors are designed to operate at 60% of full power following the loss of off-site power. They can operate at this level as long as demineralized water is available for the boilers. At Darlington and Bruce B, steam can be diverted to the condensers and recirculated to the boilers. At Pickering A and Pickering B, excess steam is vented to the atmosphere, thereby limiting the operating time to the available inventory of demineralized water.

0% Reactor Power, Hot: The successful transition from 100% to 60% power depends on several systems responding properly, and continued operation is not guaranteed. The reactor may shut down automatically through the operation of the process control systems or through the action of either of the shutdown systems.

Should a reactor shutdown occur following a load rejection, both Class IV power supplies (from the generator and the grid) to that unit will become unavailable. The main Heat Transport pumps will trip, leading to a loss of forced circulation of coolant through the core. Decay heat will be continuously removed through natural circulation

(thermosyphoning) to the boilers, and steam produced in the boilers will be exhausted to the atmosphere via atmospheric steam discharge valves. The Heat Transport System will be maintained at around 250 to 265 degrees Celsius during thermosyphoning. Standby generators will start automatically and restore Class III power to key safety-related systems. Forced circulation in the Heat Transport System will be restored once either Class III or Class IV power is available.

When shut down, the natural decay of fission products will lead to the temporary buildup of neutron absorbing elements in the fuel. If the reactor is not quickly restarted to reverse this natural process, it will "poison-out." Once poisoned-out, the reactor cannot return to operation until the fission products have further decayed, a process which typically takes up to 2 days.

Overpoisoned Guaranteed Shutdown State: In the event that certain problems are identified when reviewing the state of the reactor after a significant transient, the operating staff will cool down and depressurize the reactor, then place it in an overpoisoned guaranteed shutdown state (GSS) through the dissolution of gadolinium nitrate into the moderator. Maintenance will then be initiated to correct the problem.

Return to Service Following Loss of Grid

The return to service of a unit following any one of the above responses to a loss-of-grid event is discussed below. It is important to note that the descriptions provided relate to operations on a single unit. At multi-unit stations, the return to service of several units cannot always proceed in parallel, due to constraints on labor availability and the need to focus on critical evolutions, such as taking the reactor from a subcritical to a critical state.

60% Reactor Power: In this state, the unit can be resynchronized consistent with system demand, and power can be increased gradually to full power over approximately 24 hours.

0% Reactor Power, Hot: In this state, after approximately 2 days for the poison-out, the turbine can be run up and the unit synchronized. The reactor may shut down automatically through the operation of the process control systems or through the action of either of the shutdown systems. Thereafter, power can be increased to high power over the next day. This restart timeline does not include the time required for any repairs or maintenance that might have been necessary during the outage.

Overpoisoned Guaranteed Shutdown State: Placing the reactor in a GSS after it has been shut down requires approximately 2 days. Once the condition that required entry to the GSS is rectified, the restart requires removal of the guarantee, removal of the gadolinium nitrate through ion exchange process, heatup of the Heat Transport System, and finally synchronization to the grid. Approximately 4 days are required to complete these restart activities. In total, 6 days from shutdown are required to return a unit to service from the GSS, and this excludes any repairs that might have been required while in the GSS.

Summary of Canadian Nuclear Power Plant Response to and Safety During the August 14 Outage

On the afternoon of August 14, 2003, 15 Canadian nuclear units were operating: 13 in Ontario, 1 in Québec, and 1 in New Brunswick. Of the 13 Ontario reactors that were critical at the time of the event, 11 were operating at or near full power and 2 at low power (Pickering B Unit 7 and Pickering A Unit 4). All 13 of the Ontario reactors disconnected from the grid as a result of the grid disturbance. Seven of the 11 reactors operating at high power shut down, while the remaining 4 operated in a planned manner that enabled them to remain available to reconnect to the grid at the request of Ontario's IMO. Of the 2 Ontario reactors operating at low power, Pickering A Unit 4 tripped automatically, and Pickering B Unit 7 was tripped manually and shut down. In addition, a transient was experienced at New Brunswick Power's Point Lepreau Nuclear Generating Station, resulting in a reduction in power. Hydro Québec's Gentilly-2 nuclear station continued to operate normally as the Hydro Québec grid was not affected by the grid disturbance.

Nuclear Power Plants With Significant Transients

Pickering Nuclear Generating Station. The Pickering Nuclear Generating Station (PNGS) is located in Pickering, Ontario, on the shores of Lake Ontario, 30 kilometers east of Toronto. It houses 8 nuclear reactors, each capable of delivering 515 MW to the grid. Three of the 4 units at Pickering A (Units 1 through 3) have been shut down since late 1997. Unit 4 was restarted earlier this year following a major refurbishment and was in the process of being commissioned at the time of the event. At Pickering B, 3 units were operating at or near 100% prior to the event, and Unit 7 was

being started up following a planned maintenance outage.

Pickering A. As part of the commissioning process, Unit 4 at Pickering A was operating at 12% power in preparation for synchronization to the grid. The reactor automatically tripped on SDS1 due to Heat Transport Low Coolant Flow, when the Heat Transport main circulating pumps ran down following the Class IV power loss. The decision was then made to return Unit 4 to the guaranteed shutdown state. Unit 4 was synchronized to the grid on August 20, 2003. Units 1, 2 and 3 were in lay-up mode.

Pickering B. The Unit 5 Generator Excitation System transferred to manual control due to large voltage oscillations on the grid at 16:10 EDT and then tripped on Loss of Excitation about 1 second later (prior to grid frequency collapse). In response to the generator trip, Class IV buses transferred to the system transformer and the reactor setback. The grid frequency collapse caused the System Service Transformer to disconnect from the grid, resulting in a total loss of Class IV power. The reactor consequently tripped on the SDS1 Low Gross Flow parameter followed by an SDS2 trip due to Low Core Differential Pressure.

The Unit 6 Generator Excitation System also transferred to manual control at 16:10 EDT due to large voltage oscillations on the grid and the generator remained connected to the grid in manual voltage control. Approximately 65 seconds into the event, the grid under-frequency caused all the Class IV buses to transfer to the Generator Service Transformer. Ten seconds later, the generator separated from the Grid. Five seconds later, the generator tripped on Loss of Excitation, which caused a total loss of Class IV power. The reactor consequently tripped on the SDS1 Low Gross Flow parameter, followed by an SDS2 trip due to Low Core Differential Pressure.

Unit 7 was coming back from a planned maintenance outage and was at 0.9% power at the time of the event. The unit was manually tripped after loss of Class IV power, in accordance with procedures and returned to guaranteed shutdown state.

Unit 8 reactor automatically set back on load rejection. The setback would normally have been terminated at 20% power but continued to 2% power because of the low boiler levels. The unit subsequently tripped on the SDS1 Low Boiler Feedline Pressure parameter due to a power mismatch between the reactor and the turbine.

The following equipment problems were noted. At Pickering, the High Pressure Emergency Coolant Injection System (HPECIS) pumps are designed to operate from a Class IV power supply. As a result of the shutdown of all the operating units, the HPECIS at both Pickering A and Pickering B became unavailable for 5.5 hours. (The operating licenses for Pickering A and Pickering B permit the HPECIS to be unavailable for up to 8 hours annually. This was the first unavailability of the year.) In addition, Emergency High Pressure Service Water System restoration for all Pickering B units was delayed because of low suction pressure supplying the Emergency High Pressure Service Water pumps. Manual operator intervention was required to restore some pumps back to service.

Units were synchronized to the grid as follows: Unit 8 on August 22, Unit 5 on August 23, Unit 6 on August 25, and Unit 7 on August 29.

Darlington Nuclear Generating Station. Four reactors are located at the Darlington Nuclear Generation Station, which is on the shores of Lake Ontario in the Municipality of Clarington, 70 kilometers east of Toronto. All four of the reactors are licensed to operate at 100% of full power, and each is capable of delivering approximately 880 MW to the grid.

Unit 1 automatically stepped back to the 60% reactor power state upon load rejection at 16:12 EDT. Approval by the shift supervisor to automatically withdraw the adjuster rods could not be provided due to the brief period of time for the shift supervisor to complete the verification of systems as per procedure. The decreasing steam pressure and turbine frequency then required the reactor to be manually tripped on SDS1, as per procedure for loss of Class IV power. The trip occurred at 16:24 EDT, followed by a manual turbine trip due to under-frequency concerns.

Like Unit 1, Unit 2 automatically stepped back upon load rejection at 16:12 EDT. As with Unit 1, there was insufficient time for the shift supervisor to complete the verification of systems, and faced with decreasing steam pressure and turbine frequency, the decision was made to shut down Unit 2. Due to under-frequency on the main Primary Heat Transport pumps, the turbine was tripped manually which resulted in an SDS1 trip at 16:28 EDT.

Unit 3 experienced a load rejection at 16:12 EDT, and during the stepback Unit 3 was able to sustain operation with steam directed to the condensers.

After system verifications were complete, approval to place the adjuster rods on automatic was obtained in time to recover, at 59% reactor power.

The unit was available to resynchronize to the grid. Unit 4 experienced a load rejection at 16:12 EDT, and required a manual SDS1 trip due to the loss of Class II bus. This was followed by a manual turbine trip.

The following equipment problems were noted: Unit 4 Class II inverter trip on BUS A3 and subsequent loss of critical loads prevented unit recovery. The Unit 0 Emergency Power System BUS B135 power was lost until the Class III power was restored. (A planned battery bank B135 change out was in progress at the time of the blackout.)

Units were synchronized to the grid as follows: Unit 3 at 22:00 EDT on August 14; Unit 2 on August 17, 2003; Unit 1 on August 18, 2003; and Unit 4 on August 18, 2003.

Bruce Power. Eight reactors are located at Bruce Power on the eastern shore of Lake Huron between Kincardine and Port Elgin, Ontario. Units 5 through 8 are capable of generating 840 MW each. Presently these reactors are operating at 90% of full power due to license conditions imposed by the CNSC. Units 1 through 4 have been shutdown since December 31, 1997. Units 3 and 4 are in the process of startup.

Bruce A. Although these reactors were in guaranteed shutdown state, they were manually tripped, in accordance with operating procedures. SDS1 was manually tripped on Units 3 and 4, as per procedures for a loss of Class IV power event. SDS1 was re-poised on both units when the station power supplies were stabilized. The emergency transfer system functioned as per design, with the Class III standby generators picking up station electrical loads. The recently installed Qualified Diesel Generators received a start signal and were available to pick up emergency loads if necessary.

Bruce B. Units 5, 6, 7, and 8 experienced initial generation rejection and accompanying stepback on all four reactor units. All generators separated from the grid on under-frequency at 16:12 EDT. Units 5, 7, and 8 maintained reactor power at 60% of full power and were immediately available for reconnection to the grid.

Although initially surviving the loss of grid event, Unit 6 experienced an SDS1 trip on insufficient Neutron Over Power (NOP) margin. This occurred while withdrawing Bank 3 of the adjusters in an attempt to offset the xenon transient, resulting in a loss of Class IV power.

The following equipment problems were noted: An adjuster rod on Unit 6 had been identified on August 13, 2003, as not working correctly. Unit 6 experienced a High Pressure Recirculation Water line leak, and the Closed Loop Demineralized Water loop lost inventory to the Emergency Water Supply System.

Units were synchronized to the grid as follows: Unit 8 at 19:14 EDT on August 14, 2003; Unit 5 at 21:04 EDT on August 14; and Unit 7 at 21:14 EDT on August 14, 2003. Unit 6 was resynchronized at 02:03 EDT on August 23, 2003, after maintenance was conducted.

Point Lepreau Nuclear Generating Station. The Point Lepreau nuclear station overlooks the Bay of Fundy on the Lepreau Peninsula, 40 kilometers southwest of Saint John, New Brunswick. Point Lepreau is a single-unit CANDU 6, designed for a gross output of 680 MW. It is owned and operated by New Brunswick Power.

Point Lepreau was operating at 91.5% of full power (610 MWe) at the time of the event. When the event occurred, the unit responded to changes in grid frequency as per design. The net impact was a short-term drop in output by 140 MW, with reactor power remaining constant and excess thermal energy being discharged via the unit steam discharge valves. During the 25 seconds of the event, the unit stabilizer operated numerous times to help dampen the turbine generator speed oscillations that were being introduced by the grid frequency changes. Within 25 minutes of the event initiation, the turbine generator was reloaded to 610 MW. Given the nature of the event that occurred, there were no unexpected observations on the New Brunswick Power grid or at Point Lepreau Generating Station throughout the ensuing transient.

Nuclear Power Plants With No Transient

Gentilly-2 Nuclear Station. Hydro Québec owns and operates Gentilly-2 nuclear station, located on the south shore of the St. Lawrence River opposite the city of Trois-Rivières, Québec. Gentilly-2 is capable of delivering approximately 675 MW to Hydro Québec's grid. The Hydro Québec grid was not affected by the power system outage and Gentilly-2 continued to operate normally.

General Observations Based on the Facts Found During Phase One

Following the review of the data provided by the Canadian nuclear power plants, the Nuclear Working Group concludes the following:

- None of the reactor operators had any advanced warning of impending collapse of the grid.
- Canadian nuclear power plants did not trigger the power system outage or contribute to its spread.
- There were no risks to the health and safety of workers or the public as a result of the concurrent shutdown of several reactors. Automatic safety systems for the turbine generators and reactors worked as designed. (See Table 7.2 for a summary of shutdown events for Canadian nuclear power plants.)

The NWG also identified the following secondary issues:

- Equipment problems and design limitations at Pickering B resulted in a temporary reduction in the effectiveness of some of the multiple safety barriers, although the equipment failure was within the unavailability targets found in the OP&Ps approved by the CNSC as part of Ontario Power Generation's license.
- Existing OP&Ps place constraints on the use of adjuster rods to respond to events involving rapid reductions in reactor power. While greater flexibility with respect to use of adjuster rods would not have prevented the shutdown, some units, particularly those at Darlington, might have been able to return to service less than 1 hour after the initiating event.
- Off-site power was unavailable for varying periods of time, from approximately 3 hours at Bruce B to approximately 9 hours at Pickering A. Despite the high priority assigned by the IMO to restoring power to the nuclear stations, the stations had some difficulty obtaining timely information about the status of grid recovery and the restoration of Class IV power. This information is important for Ontario Power Generation's and Bruce Power's response strategy.
- Required regulatory approvals from CNSC staff were obtained quickly and did not delay the restart of the units; however, CNSC staff was unable to immediately activate the CNSC's Emergency Operation Centre because of loss of power to the CNSC's head office building. CNSC staff, therefore, established communications with licensees and the U.S. NRC from other locations.

Table 7.2. Summary of Shutdown Events for Canadian Nuclear Power Plants

Generating Station	Unit	Operating Status at Time of Event			Response to Event			
		Full Power	Startup	Not Operating	Stepback to 60% Power, Available To Supply Grid	Turbine Trip	Reactor Trip	
							SDS1	SDS2
Pickering NGS	1			√			(a)	
	2			√				
	3			√				
	4		√				√	(b)
	5	√					√	√
	6	√					√	√
	7		√				√	
	8	√					√	
Darlington NGS	1	√				√	√	
	2	√				√	√	
	3	√			√			
	4	√				√	√	
Bruce Nuclear Power Development	1			√				
	2			√				
	3			√			√	
	4			√			√	
	5	√			√			
	6	√					√	
	7	√			√			
	8	√			√			

[a] Pickering A Unit 1 tripped as a result of electrical bus configuration immediately prior to the event which resulted in a temporary loss of Class II power.

[b] Pickering A Unit 4 also tripped on SDS-E.

Notes: Unit 7 at Pickering B was operating at low power, warming up prior to reconnecting to the grid after a maintenance outage. Unit 4 at Pickering A was producing at low power, as part of the reactor’s commissioning after extensive refurbishment since being shut down in 1997.

8. Physical and Cyber Security Aspects of the Blackout

Summary

The objective of the Security Working Group (SWG) is to determine what role, if any, that a malicious cyber event may have played in causing, or contributing to, the power outage of August 14, 2003. Analysis to date provides no evidence that malicious actors are responsible for, or contributed to, the outage. The SWG acknowledges reports of al-Qaeda claims of responsibility for the power outage of August 14, 2003; however, those claims are not consistent with the SWG's findings to date. There is also no evidence, nor is there any information suggesting, that viruses and worms prevalent across the Internet at the time of the outage had any significant impact on power generation and delivery systems. SWG analysis to date has brought to light certain concerns with respect to: the possible failure of alarm software; links to control and data acquisition software; and the lack of a system or process for some operators to view adequately the status of electric systems outside their immediate control.

Further data collection and analysis will be undertaken by the SWG to test the findings detailed in this interim report and to examine more fully the cyber security aspects of the power outage. The outcome of Electric System Working Group (ESWG) root cause analysis will serve to focus this work. As the significant cyber events are identified by the ESWG, the SWG will examine them from a security perspective.

Security Working Group: Mandate and Scope

It is widely recognized that the increased reliance on information technology (IT) by critical infrastructure sectors, including the energy sector, has increased their vulnerability to disruption via cyber means. The ability to exploit these vulnerabilities has been demonstrated in North America. The SWG was established to address the cyber-related aspects of the August 14, 2003, power outage. The SWG is made up of U.S. and Canadian Federal, State, Provincial, and local experts in both physical and cyber security. For the purposes of its work, the SWG has defined a "malicious cyber event" as the manipulation of data, software or hardware for the purpose of deliberately disrupting the systems that control and support the generation and delivery of electric power.

The SWG is working closely with the U.S. and Canadian law enforcement, intelligence, and homeland security communities to examine the possible role of malicious actors in the power outage of August 14, 2003. A primary activity to date has been the collection and review of available intelligence that may relate to the outage.

The SWG is also collaborating with the energy industry to examine the cyber systems that control power generation and delivery operations, the physical security of cyber assets, cyber policies and procedures, and the functionality of supporting infrastructures-such as communication systems and backup power generation, which facilitate the smooth-running operation of cyber assets-to determine whether the operation of these systems was affected by malicious activity. The collection of information along these avenues of inquiry is ongoing.

The SWG is coordinating its efforts with those of the other Working Groups, and there is a significant interdependence on the work products and findings of each group. The SWG's initial focus is on the cyber operations of those companies in the United States involved in the early stages of the power outage timeline, as identified by the ESWG. The outcome of ESWG analysis will serve to identify key events that may have caused, or contributed to, the outage. As the significant cyber events are identified, the SWG will examine them from a security perspective. The amount of information for analysis is identified by the ESWG as pertinent to the SWG's analysis is considerable.

Examination of the physical, non-cyber infrastructure aspects of the power outage of August 14, 2003, is outside the scope of the SWG's analysis.

Nevertheless, if a breach of physical security unrelated to the cyber dimensions of the infrastructure comes to the SWG's attention during the course of the work of the Task Force, the SWG will conduct the necessary analysis.

Also outside the scope of the SWG's work is analysis of the cascading impacts of the power outage on other critical infrastructure sectors. Both the Canadian Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) and the U.S. Department of Homeland Security (DHS) are examining these issues, but not within the context of the Task Force. The SWG is closely coordinating its efforts with OCIPEP and DHS.

Cyber Security in the Electricity Sector

The generation and delivery of electricity has been, and continues to be, a target of malicious groups and individuals intent on disrupting the electric power system. Even attacks that do not directly target the electricity sector can have disruptive effects on electricity system operations. Many malicious code attacks, by their very nature, are unbiased and tend to interfere with operations supported by vulnerable applications. One such incident occurred in January 2003, when the "Slammer" Internet worm took down monitoring computers at FirstEnergy Corporation's idled Davis-Besse nuclear plant. A subsequent report by the North American Electric Reliability Council (NERC) concluded that, although it caused no outages, the infection blocked commands that operated other power utilities. The report, "NRC Issues Information Notice on Potential of Nuclear Power Plant Network to Worm Infection," is available at web site http://www.nrc.gov/reading-rm/doc-collections/news/2003/03-108.html.

This example, among others, highlights the increased vulnerability to disruption via cyber means faced by North America's critical infrastructure sectors, including the energy sector. Of specific concern to the U.S. and Canadian governments are the Supervisory Control and Data Acquisition (SCADA) systems, which contain computers and applications that perform a wide variety of functions across many industries. In electric power, SCADA includes telemetry for status and control, as well as Energy Management Systems (EMS), protective relaying, and automatic generation control. SCADA systems were developed to maximize functionality and interoperability, with little attention given to cyber security. These systems, many of which were intended to be isolated, are now, for a variety of business and operational reasons, either directly or indirectly connected to the global Internet. For example, in some instances, there may be a need for employees to monitor SCADA systems remotely. However, connecting SCADA systems to a remotely accessible computer network can present security risks. These risks include the compromise of sensitive operating information and the threat of unauthorized access to SCADA systems' control mechanisms.

Security has always been a priority for the electricity sector in North America; however, it is a greater priority now than ever before. Electric system operators recognize that the threat environment is changing and that the risks are greater than in the past, and they have taken steps to improve their security postures. NERC's Critical Infrastructure Protection Advisory Group has been examining ways to improve both the physical and cyber security dimensions of the North American power grid. This group includes Canadian and U.S. industry experts in the areas of cyber security, physical security and operational security. The creation of a national SCADA program to improve the physical and cyber security of these control systems is now also under discussion in the United States. The Canadian Electrical Association Critical Infrastructure Working Group is examining similar measures.

Information Collection and Analysis

In addition to analyzing information already obtained from stakeholder interviews, telephone transcripts, law enforcement and intelligence information, and other ESWG working documents, the SWG will seek to review and analyze other sources of data on the cyber operations of those companies in the United States involved in the early stages of the power outage timeline, as identified by the ESWG. Available information includes log data from routers, intrusion detection systems, firewalls, and EMS; change management logs; and physical security materials. Data are currently being collected, in collaboration with the private sector and with consideration toward its protection from further disclosure where there are proprietary or national security concerns.

The SWG is divided into six sub-teams to address the discrete components of this investigation: Cyber Analysis, Intelligence Analysis, Physical Analysis, Policies and Procedures, Supporting Infrastructure, and Root Cause Liaison. The SWG organized itself in this manner to create a holistic approach to each of the main areas of concern with regard to power grid vulnerabilities. Rather than analyze each area of concern separately, the SWG sub-team structure provides a more comprehensive framework in which to investigate whether malicious activity was a cause of the power outage of August 14, 2003. Each sub-team is staffed with Subject Matter Experts (SMEs) from government, industry, and academia to provide the analytical breadth and depth necessary to complete its objective. A detailed overview of the sub-team structure and activities, those planned and those taken, for each sub-team is provided below.

Cyber Analysis

The Cyber Analysis sub-team is led by the CERT® Coordination Center (CERT/CC) at Carnegie Mellon University and the Royal Canadian Mounted Police (RCMP). This team is focused on analyzing and reviewing the electronic media of computer networks in which online communications take place. The sub-team is examining these networks to determine whether they were maliciously used to cause, or contribute to, the August 14 outage. It is specifically reviewing the existing cyber topology, cyber logs, and EMS logs. The team is also conducting interviews with vendors to identify known system flaws and vulnerabilities. The sub-team is collecting, processing, and synthesizing data to determine whether a malicious cyber-related attack was a direct or indirect cause of the outage.

This sub-team has taken a number of steps in recent weeks, including reviewing NERC reliability standards to gain a better understanding of the overall security posture of the electric power industry. Additionally, the sub-team participated in meetings in Baltimore on August 22 and 23, 2003. The meetings provided an opportunity for the cyber experts and the power industry experts to understand the details necessary to conduct an investigation. The cyber data retention request was produced during this meeting.

Members of the sub-team also participated in the NERC/Department of Energy (DOE) Fact Finding meeting held in Newark, New Jersey, on September 8, 2003. Each company involved in the outage provided answers to a set of questions related to the outage. The meeting helped to provide a better understanding of what each company experienced before, during, and after the outage. Additionally, sub-team members participated in interviews with the control room operators from FirstEnergy on October 8 and 9, 2003, and from Cinergy on October 10, 2003. These interviews have identified several key areas for further discussion.

The Cyber Analysis sub-team continues to gain a better understanding of events on August 14, 2003. Future analysis will be driven by information received from the ESWG's Root Cause Analysis sub-team and will focus on:

- Conducting additional interviews with control room operators and IT staff from the key companies involved in the outage.
- Conducting interviews with the operators and IT staff responsible for the NERC Interchange Distribution Calculator system. Some reports indicate that this system may have been unavailable during the time of the outage.
- Conducting interviews with key vendors for the EMS.
- Analyzing the configurations of routers, firewalls, intrusion detection systems, and other network devices to get a better understanding of potential weaknesses in the control system cyber defenses.
- Analyzing logs and other information for signs of unauthorized activity.

Intelligence Analysis

The Intelligence Analysis sub-team is led by DHS and the RCMP, which are working closely with Federal, State, and local law enforcement, intelligence, and homeland security organizations to assess whether the power outage was the result of a malicious attack. Preliminary analysis provides no evidence that malicious actors-either individuals or organizations-are responsible for, or contributed to, the power outage of August 14, 2003. Additionally, the sub-team has found no indication of deliberate physical damage to power generating stations and delivery lines on the day of the outage, and there are no reports indicating that the power outage was caused by a computer network attack.

Both U.S. and Canadian government authorities provide threat intelligence information to their respective energy sectors when appropriate. No

intelligence reports before, during, or after the power outage indicated any specific terrorist plans or operations against the energy infrastructure. There was, however, threat information of a general nature relating to the sector, which was provided to the North American energy industry by U.S. and Canadian government agencies in late July 2003. This information indicated that al-Qaeda might attempt to carry out a physical attack involving explosions at oil production facilities, power plants, or nuclear plants on the U.S. East Coast during the summer of 2003. The type of physical attack described in the intelligence that prompted this threat warning is not consistent with the events of the power outage; there is no indication of a kinetic event before, during, or immediately after the August 14 outage.

Despite all the above indications that no terrorist activity caused the power outage, al-Qaeda did publicly claim responsibility for its occurrence:

- **August 18, 2003:** Al-Hayat, an Egyptian media outlet, published excerpts from a communiqué attributed to al-Qaeda. Al Hayat claimed to have obtained the communiqué from the website of the International Islamic Media Center. The content of the communiqué asserts that the "brigades of Abu Fahes Al Masri had hit two main power plants supplying the East of the U.S., as well as major industrial cities in the U.S. and Canada, 'its ally in the war against Islam (New York and Toronto) and their neighbors.'" Furthermore, the operation "was carried out on the orders of Osama bin Laden to hit the pillars of the U.S. economy," as "a realization of bin Laden's promise to offer the Iraqi people a present." The communiqué does not specify the way in which the alleged sabotage was carried out, but it does elaborate on the alleged damage to the U.S. economy in the areas of finance, transportation, energy, and telecommunications.

Additional claims and commentary regarding the power outage appeared in various Middle Eastern media outlets:

- **August 26, 2003:** A conservative Iranian daily newspaper published a commentary regarding the potential of computer technology as a tool for terrorists against infrastructures dependent on computer networks-most notably, water, electric, public transportation, trade organizations, and "supranational companies" in the United States.
- **September 4, 2003:** An Islamist participant in a Jihadist chat room forum claimed that sleeper cells associated with al-Qaeda used the power outage as a cover to infiltrate the United States from Canada.

These claims above, as known, are not consistent with the SWG's findings to date. They are also not consistent with recent congressional testimony by the U.S. Federal Bureau of Investigation (FBI). Larry A. Mefford, Executive Assistant Director in charge of the FBI's Counterterrorism and Counterintelligence programs, testified to the U.S. Congress on September 4, 2003, that, "To date, we have not discovered any evidence indicating that the outage was a result of activity by international or domestic terrorists or other criminal activity." He also testified that, "The FBI has received no specific, credible threats to electronic power grids in the United States in the recent past and the claim of the Abu Hafs al-Masri Brigade to have caused the blackout appears to be no more than wishful thinking. We have no information confirming the actual existence of this group." Mr. Mefford's Statement for the Record is available at web site http://www.fbi.gov/congress/congress03/mefford090403.htm.

Current assessments suggest that there are terrorists and other malicious actors who have the capability to conduct a malicious cyber attack with potential to disrupt the energy infrastructure. Although such an attack cannot be ruled out entirely, an examination of available information and intelligence does not support any claims of a deliberate attack against the energy infrastructure on, or leading up to, August 14, 2003. The few instances of physical damage that occurred on power delivery lines were the result of natural acts and not of sabotage. No intelligence reports before, during, or after the power outage indicate any specific terrorist plans or operations against the energy infrastructure. No incident reports detail suspicious activity near the power generation plants or delivery lines in question.

Physical Analysis

The Physical Analysis sub-team is led by the U.S. Secret Service and the RCMP. These organizations have particular expertise in physical security assessments in the energy sector. The sub-team is focusing on issues related to how the cyber-related facilities of the energy sector companies are secured, including the physical integrity of data centers and control rooms, along with security procedures and policies used to limit access to sensitive areas. Focusing on the facilities identified as having a causal relationship to the outage,

the sub-team is seeking to determine whether the physical integrity of the cyber facilities was breached, either externally or by an insider, before or during the outage; and if so, whether such a breach caused or contributed to the power outage. Although the sub-team has analyzed information provided to both the EWG and the Nuclear Working Group (NWG), the Physical Analysis sub-team is also reviewing information resulting from recent face-to-face meetings with energy sector personnel and site visits to energy sector facilities, to determine the physical integrity of the cyber infrastructure.

The sub-team has compiled a list of questions covering location, accessibility, cameras, alarms, locks, and fire protection and water systems as they apply to computer server rooms. Based on discussions of these questions during its interviews, the sub-team is in the process of ascertaining whether the physical integrity of the cyber infrastructure was breached. Additionally, the sub-team is examining access and control measures used to allow entry into command and control facilities and the integrity of remote facilities.

The sub-team is also concentrating on mechanisms used by the companies to report unusual incidents within server rooms, command and control rooms, and remote facilities. The sub-team is also addressing the possibility of an insider attack on the cyber infrastructure.

Policies and Procedures

The Policies and Procedures sub-team is led by DHS and OCIPEP, which have personnel with strong backgrounds in the fields of electric delivery operations, automated control systems (including SCADA and EMS), and information security. The sub-team is focused on examining the overall policies and procedures that may or may not have been in place during the events leading up to and during the August 14 power outage. The team is examining policies that are centrally related to the cyber systems of the companies identified in the early stages of the power outage. Of specific interest are policies and procedures regarding the upgrade and maintenance (to include system patching) of the command and control (C2) systems, including SCADA and EMS. Also of interest are the procedures for contingency operations and restoration of systems in the event of a computer system failure or a cyber event, such as an active hack or the discovery of malicious code. The group is conducting further interviews and is continuing its analysis to build solid conclusions about the policies and procedures relating to the outage.

Supporting Infrastructure

The Supporting Infrastructure sub-team is led by a DHS expert with experience assessing supporting infrastructure elements such as water cooling for computer systems, backup power systems, heating, ventilation and air conditioning (HVAC), and supporting telecommunications networks. OCIPEP is the Canadian co-lead for this effort. The sub-team is analyzing the integrity of the supporting infrastructure and its role, if any, in the August 14 power outage, and whether the supporting infrastructure was performing at a satisfactory level before and during the outage. In addition, the team is contacting vendors to determine whether there were maintenance issues that may have affected operations during or before the outage.

The sub-team is focusing specifically on the following key issues in visits to each of the designated electrical entities:

- Carrier/provider/vendor for the supporting infrastructure services and/or systems at select company facilities
- Loss of service before and/or after the power outage
- Conduct of maintenance activities before and/or after the power outage
- Conduct of installation activities before and/or after the power outage
- Conduct of testing activities before and/or after the power outage
- Conduct of exercises before and/or after the power outage
- Existence of a monitoring process (log, checklist, etc.) to document the status of supporting infrastructure services.

Root Cause Analysis

The SWG Root Cause Liaison sub-team (SWG/RC) has been following the work of the ESWG to identify potential root causes of the power outage. As these root cause elements are identified, the sub-team will assess with the ESWG any potential linkages to physical and/or cyber malfeasance.

The root cause analysis work of the ESWG is still in progress; however, the initial analysis has

found no causal link between the power outage and malicious activity, whether physical or cyber initiated. Root cause analysis for an event like the August 14 power outage involves a detailed process to develop a hierarchy of actions and events that suggest causal factors. The process includes: development of a detailed timeline of the events, examination of actions related to the events, and an assessment of factors that initiated or exacerbated the events. An assessment of the impact of physical security as a contributor to the power outage is conditional upon discovery of information suggesting that a malicious physical act initiated or exacerbated the power outage. There are no such indications thus far, and no further assessment by the SWG in this area is indicated.

Cyber Timeline

The following sequence of events was derived from discussions with representatives of FirstEnergy and the Midwest Independent Transmission System Operator (MISO). All times are approximate and will need to be confirmed by an analysis of company log data.

- The first significant cyber-related event of August 14, 2003, occurred at 12:40 EDT at the MISO. At this time, a MISO EMS engineer purposely disabled the automatic periodic trigger on the State Estimator (SE) application, which allows MISO to determine the real-time state of the power system for its region. Disabling of the automatic periodic trigger, a program feature that causes the SE to run automatically every 5 minutes, is a necessary operating procedure when resolving a mismatched solution produced by the SE. The EMS engineer determined that the mismatch in the SE solution was due to the SE model depicting Cinergy's Bloomington-Denois Creek 230-kV line as being in service, when it had actually been out of service since 12:12 EDT.
- At 13:00 EDT, after making the appropriate changes to the SE model and manually triggering the SE, the MISO EMS engineer achieved two valid solutions.
- At 13:30 EDT, the MISO EMS engineer went to lunch. He forgot to re-engage the automatic periodic trigger.
- At 14:14 EDT, FirstEnergy's "Alarm and Event Processing Routine" (AEPR)-a key software program that gives operators visual and audible indications of events occurring on their portion of the grid-began to malfunction. FirstEnergy system operators were unaware that the software was not functioning properly. This software did not become functional again until much later that evening.
- At 14:40 EDT, an Ops engineer discovered that the SE was not solving. He went to notify an EMS engineer.
- At 14:41 EDT, FirstEnergy's server running the AEPR software failed to the backup server. Control room staff remained unaware that the AEPR software was not functioning properly.
- At 14:44 EDT, an MISO EMS engineer, after being alerted by the Ops engineer, reactivated the automatic periodic trigger and, for speed, manually triggered the program. The SE program again showed a mismatch.
- At 14:54 EDT, FirstEnergy's backup server failed. AEPR continued to malfunction. The Area Control Error (ACE) calculations and Strip Charting routines malfunctioned, and the dispatcher user interface slowed significantly.
- At 15:00 EDT, FirstEnergy used its emergency backup system to control the system and make ACE calculations. ACE calculations and control systems continued to run on the emergency backup system until roughly 15:08 EDT, when the primary server was restored.
- At 15:05 EDT, FirstEnergy's Harding-Chamberlin 345-kV line tripped and locked out. FE system operators did not receive notification from the AEPR software, which continued to malfunction, unbeknownst to the FE system operators.
- At 15:08 EDT, using data obtained at roughly 15:04 EDT (it takes about 5 minutes for the SE to provide a result), the MISO EMS engineer concluded that the SE mismatched due to a line outage. His experience allowed him to isolate the outage to the Stuart-Atlanta 345-kV line (which tripped about an hour earlier, at 14:02 EDT). He took the Stuart-Atlanta line out of service in the SE model and got a valid solution.
- Also at 15:08 EDT, the FirstEnergy primary server was restored. ACE calculations and control systems were now running on the primary server. AEPR continued to malfunction, unbeknownst to the FirstEnergy system operators.
- At 15:09 EDT, the MISO EMS engineer went to the control room to tell the operators that he thought the Stuart-Atlanta line was out of service. Control room operators referred to their

"Outage Scheduler" and informed the EMS engineer that their data showed the Stuart-Atlanta line was "up" and that the EMS engineer should depict the line as in service in the SE model. At 15:17 EDT, the EMS engineer ran the SE with the Stuart-Atlanta line "live." The model again mismatched.

- At 15:29 EDT, the MISO EMS Engineer asked MISO operators to call the PJM Interconnect to determine the status of the Stuart-Atlanta line. MISO was informed that the Stuart-Atlanta line had tripped at 14:02 EDT. The EMS engineer adjusted the model, which by that time had been updated with the 15:05 EDT Harding-Chamberlin 345-kV line trip, and came up with a valid solution.
- At 15:32 EDT, FirstEnergy's Hanna-Juniper 345-kV line tripped and locked out. The AEPR continued to malfunction.
- At 15:41 EDT, the lights flickered at FirstEnergy's control facility, because the facility had lost grid power and switched over to its emergency power supply.
- At 15:42 EDT, a FirstEnergy dispatcher realized that the AEPR was not working and informed technical support staff of the problem.

Findings to Date

The SWG has developed the following findings via analysis of collected data and discussions with energy companies and entities identified by the ESWG as pertinent to the SWG's analysis. SWG analysis to date provides no evidence that malicious actors-either individuals or organizations-are responsible for, or contributed to, the power outage of August 14, 2003. The SWG continues to coordinate closely with the other Task Force Working Groups and members of the U.S. and Canadian law enforcement and DHS/OCIPEP communities to collect and analyze data to test this preliminary finding.

No intelligence reports before, during, or after the power outage indicated any specific terrorist plans or operations against the energy infrastructure. There was, however, threat information of a general nature related to the sector, which was provided to the North American energy industry by U.S. and Canadian government agencies in late July 2003. This information indicated that al-Qaeda might attempt to carry out a physical attack against oil production facilities, power plants, or nuclear plants on the U.S. East Coast during the summer of 2003. The type of physical attack described in the intelligence that prompted the threat information was not consistent with the events of the power outage.

Although there were a number of worms and viruses impacting the Internet and Internet-connected systems and networks in North America before and during the outage, the SWG's preliminary analysis provides no indication that worm/virus activity had a significant effect on the power generation and delivery systems. Further SWG analysis will test this finding.

SWG analysis to date suggests that failure of a software program-not linked to malicious activity-may have contributed significantly to the power outage of August 14, 2003. Specifically, key personnel may not have been aware of the need to take preventive measures at critical times, because an alarm system was malfunctioning. The SWG continues to work closely with the operators of the affected system to determine the nature and scope of the failure, and whether similar software failures could create future system vulnerabilities. The SWG is in the process of engaging system vendors and operators to determine whether any technical or process-related modifications should be implemented to improve system performance in the future.

The existence of both internal and external links from SCADA systems to other systems introduced vulnerabilities. At this time, however, preliminary analysis of information derived from interviews with operators provides no evidence indicating exploitation of these vulnerabilities before or during the outage. Future SWG work will provide greater insight into this issue.

Analysis of information derived from interviews with operators suggests that, in some cases, visibility into the operations of surrounding areas was lacking. Some companies appear to have had only a limited understanding of the status of the electric systems outside their immediate control. This may have been, in part, the result of a failure to use modern dynamic mapping and data sharing systems. Future SWG work will clarify this issue.

Appendix A

Description of Outage Investigation and Plan for Development of Recommendations

On August 14, 2003, the northeastern U.S. and Ontario, Canada, suffered one of the largest power blackouts in the history of North America. The area affected extended from New York, Massachusetts, and New Jersey west to Michigan, and from Ohio north to Ontario.

This appendix outlines the process used to investigate why the blackout occurred and was not contained, and explains how recommendations will be developed to prevent and minimize the scope of future outages. The essential first step in the process was the creation of a joint U.S.-Canada Power System Outage Task Force to provide oversight for the investigation and the development of recommendations.

Task Force Composition and Responsibilities

President George W. Bush and Prime Minister Jean Chrétien created the joint Task Force to identify the causes of the August 14, 2003 power outage and to develop recommendations to prevent and contain future outages. The co-chairs of the Task Force are U.S. Secretary of Energy Spencer Abraham and Minister of Natural Resources Canada Herb Dhaliwal. Other U.S. members are Nils J. Diaz, Chairman of the Nuclear Regulatory Commission, Tom Ridge, Secretary of Homeland Security, and Pat Wood, Chairman of the Federal Energy Regulatory Commission. The other Canadian members are Deputy Prime Minister John Manley, Linda J. Keen, President and CEO of the Canadian Nuclear Safety Commission, and Kenneth Vollman, Chairman of the National Energy Board. The coordinators for the Task Force are Jimmy Glotfelty on behalf of the U.S. Department of Energy and Dr. Nawal Kamel on behalf of Natural Resources Canada.

U.S. Energy Secretary Spencer Abraham and Minister of Natural Resources Canada Herb Dhaliwal met in Detroit, Michigan on August 20, and agreed on an outline for the Task Force's activities. The outline directed the Task Force to divide its efforts into two phases. The first phase was to focus on what caused the outage and why it was not contained, and the second was to focus on the development of recommendations to prevent and minimize future power outages. On August 27, Secretary Abraham and Minister Dhaliwal announced the formation of three Working Groups to support the work of the Task Force. The three Working Groups address electric system issues, security matters, and questions related to the performance of nuclear power plants over the course of the outage. The members of the Working Groups are officials from relevant federal departments and agencies, technical experts, and senior representatives from the affected states and the Province of Ontario.

U.S.-Canada-NERC Investigation Team

Under the oversight of the Task Force, a team of electric system experts was established to investigate the causes of the outage. This team was comprised of individuals from several U.S. federal agencies, the U.S. Department of Energy's national laboratories, Canadian electric industry, Canada's National Energy Board, staff from the North American Electric Reliability Council (NERC), and the U.S. electricity industry. The overall investigative team was divided into several analytic groups with specific responsibilities, including data management, determining the sequence of outage events, system modeling, evaluation of operating tools and communications, transmission system performance, generator performance, vegetation and right-of-way management, transmission and reliability investments, and root cause analysis. The root cause analysis is best understood as an analytic framework as opposed to a stand-alone analytic effort. Its function was to enable the analysts to draw upon and organize information from all of the other analyses, and by means of a rigorously logical and systematic procedure, assess alternative hypotheses and identify the root causes of the outage.

Separate teams were established to address issues related to the performance of nuclear power plants affected by the outage, and physical and cyber security issues related to the bulk power infrastructure.

Function of the Working Groups

The U.S. and Canadian co-chairs of each of the three Working Groups (i.e., an Electric System Working Group, a Nuclear Working Group, and a Security Working Group) designed various work products to be prepared by the investigative teams. Drafts of these work products were reviewed and commented upon by the relevant Working Groups. These work products were then synthesized into a single Interim Report reflecting the conclusions of the three investigative teams and the Working Groups. Determination of when the Interim Report was complete and appropriate for release to the public was the responsibility of the joint Task Force.

Confidentiality of Data and Information

Given the seriousness of the blackout and the importance of averting or minimizing future blackouts, it was essential that the Task Force's teams have access to pertinent records and data from the regional independent system operators (ISOs) and electric companies affected by the blackout, and for the investigative team to be able to interview appropriate individuals to learn what they saw and knew at key points in the evolution of the outage, what actions they took, and with what purpose. In recognition of the sensitivity of this information, Working Group members and members of the teams signed agreements affirming that they would maintain the confidentiality of data and information provided to them, and refrain from independent or premature statements to the media or the public about the activities, findings, or conclusions of the individual Working Groups or the Task Force as a whole.

Relevant U.S. and Canadian Legal Framework

United States

The Secretary of Energy directed the Department of Energy (DOE) to gather information and conduct an investigation to examine the cause or causes of the August 14, 2003 blackout. In initiating this effort, the Secretary exercised his authority, including section 11 of the Energy Supply and Environmental Coordination Act of 1974, and section 13 of the Federal Energy Administration Act of 1974, to gather energy-related information and conduct investigations. This authority gives him and the DOE the ability to collect such energy information as he deems necessary to assist in the formulation of energy policy, to conduct investigations at reasonable times and in a reasonable manner, and to conduct physical inspections at energy facilities and business premises. In addition, DOE can inventory and sample any stock of fuels or energy sources therein, inspect and copy records, reports, and documents from which energy information has been or is being compiled and to question such persons as it deems necessary. DOE worked closely with the Canadian Department of Natural Resources and NERC on the investigation.

Canada

Minister Dhaliwal, as the Minister responsible for Natural Resources Canada, was appointed by Prime Minister Chrétien as the Canadian Co-Chair of the Task Force. Minister Dhaliwal works closely with his American Co-Chair, Secretary of Energy Abraham, as well as NERC and his provincial counterparts in carrying out his responsibilities. The Task Force will report to the Prime Minister and the US President upon the completion of its mandate.

Under Canadian law, the Task Force is characterized as a non-statutory, advisory body that does not have independent legal personality. The Task Force does not have any power to compel evidence or witnesses, nor is it able to conduct searches or seizures. In Canada, the Task Force will rely on voluntary disclosure for obtaining information pertinent to its work.

Investigative Process

Collection of Data and Information from ISOs, Utilities, States, and the Province of Ontario

On Tuesday, August 19, 2003, investigators affiliated with the U.S. Department of Energy (USDOE) began interviewing control room operators and other key officials at the ISOs and the companies most directly involved with the initial stages of the outage. In addition to the information gained in the interviews, the interviewers sought information and data about control room operations and practices, the organization's system status and conditions on August 14, the organization's operating procedures and guidelines, load limits on its system, emergency planning and procedures, system security analysis tools and procedures, and practices for voltage and frequency monitoring. Similar interviews were held later with staff at Ontario's Independent Electricity Market Operator (IMO) and Hydro One in Canada.

On August 22 and 26, NERC directed the reliability coordinators at the ISOs to obtain a wide range of data and information from the control area coordinators under their oversight. The data requested included System Control and Data Acquisition (SCADA) logs, Energy Management System (EMS) logs, alarm logs, data from local digital fault recorders, data on transmission line and generator "trips" (i.e., automatic disconnection to prevent physical damage to equipment), state estimator data, operator logs and transcripts, and information related to the operation of capacitors, phase shifting transformers, load shedding, static var compensators, special protection schemes or stability controls, and high-voltage direct current (HVDC) facilities. NERC issued another data request to FirstEnergy on September 15 for copies of studies since 1990 addressing voltage support, reactive power supply, static capacitor applications, voltage requirements, import or transfer capabilities (in relation to reactive capability or voltage levels), and system impacts associated with unavailability of the Davis-Besse plant. All parties were instructed that data and information provided to either DOE or NERC did not have to be submitted a second time to the other entity—all material provided would go into a common data base.

The investigative team held three technical conferences (August 22, September 8-9, and October 1-3) with the ISOs and key utilities aimed at clarifying the data received, filling remaining gaps in the data, and developing a shared understanding of the data's implications. The team also requested information from the public utility commissions in the affected states and Ontario on transmission right-of-way maintenance, transmission planning, and the scope of any state-led investigations concerning the August 14 blackout. The team also commissioned a study by a firm specializing in utility vegetation management to identify "best practices" concerning such management in right of way areas and to use those practices in gauging the performance of companies who had lines go out of service on August 14 due to tree contact.

Data "Warehouse"

The data collected by the investigative team became voluminous, so an electronic repository capable of storing thousands of transcripts, graphs, generator and transmission data and reports was constructed in Princeton, NJ at the NERC headquarters. At present the data base is over 20 Gigabytes of information. That data consists of over 10,000 different files some of which contain multiple files. The objective was to establish a set of validated databases that the several analytic teams could access independently on an as-needed basis.

The following are the information sources for the Electric System Investigation:

- Interviews conducted by members of the U.S.-Canada Electric Power System Outage Investigation Team with personnel at all of the utilities, control areas and reliability coordinators in the weeks following the blackout.
- Three fact-gathering meetings conducted by the Investigation Team with personnel from the above organizations on August 22, September 8 and 9, and October 1 to 3, 2003.
- Materials provided by the above organizations in response to one or more data requests from the Investigation Team.
- Extensive review of all taped phone transcripts between involved operations centers.
- Additional interviews and field visits with operating personnel on specific issues in October, 2003.
- Field visits to examine transmission lines and vegetation at short-circuit locations.
- Materials provided by utilities and state regulators in response to data requests on vegetation management issues.
- Detailed examination of thousands of individual relay trips for transmission and generation events.
- Computer simulation and modeling conducted by groups of experts from utilities, reliability coordinators, reliability councils, and the U.S. and Canadian governments.

Sequence of Events

Establishing a precise and accurate sequence of outage-related events was a critical building block for the other parts of the investigation. One of the key problems in developing this sequence was that although much of the data pertinent to an event was time-stamped, there was some variance from source to source in how the time-stamping was done, and not all of the time-stamps were synchronized to the National Institute of Standards and Technology (NIST) standard clock in Boulder, CO. Validating the timing of specific events

became a large, important, and sometimes difficult task. This work was also critical to the issuance by the Task Force on September 12 of a "timeline" for the outage. The timeline briefly described the principal events, in sequence, leading up to the initiation of the outage's cascade phase, and then in the cascade itself. The timeline was not intended, however, to address the causal relationships among the events described, or to assign fault or responsibility for the blackout. All times in the chronology are in Eastern Daylight Time.

System Modeling and Simulation Analysis

The system modeling and simulation team replicated system conditions on August 14 and the events leading up to the blackout. While the sequence of events provides a precise description of discrete events, it does not describe the overall state of the electric system and how close it was to various steady-state, voltage stability, and power angle stability limits. An accurate computer model of the system, benchmarked to actual conditions at selected critical times on August 14, allowed analysts to conduct a series of sensitivity studies to determine if the system was stable and within limits at each point in time leading up to the cascade. The analysis also confirmed when the system became unstable, and allowed analysts to test whether measures such as load-shedding would have prevented the cascade.

This team consisted of a number of NERC staff and persons with expertise in areas necessary to read and interpret all of the data logs, digital fault recorder information, sequence of events recorders information, etc. The team consisted of about 36 people involved at various different times with additional experts from the affected areas to understand the data.

Assessment of Operations Tools, SCADA/EMS, Communications, and Operations Planning

The Operations Tools, SCADA/EMS, Communications, and Operations Planning Team assessed the observability of the electric system to operators and reliability coordinators, and the availability and effectiveness of operational (real-time and day-ahead) reliability assessment tools, including redundancy of views and the ability to observe the "big picture" regarding bulk electric system conditions. The team investigated operating practices and effectiveness of operating entities and reliability coordinators in the affected area. This team investigated all aspects of the blackout related to operator and reliability coordinator knowledge of system conditions, action or inactions, and communications.

Frequency/ACE Analysis

The Frequency/ACE Team analyzed potential frequency anomalies that may have occurred on August 14, as compared to typical interconnection operations. The team also determined whether there were any unusual issues with control performance and frequency and any effects they may have had related to the cascading failure, and whether frequency related anomalies were contributing factors or symptoms of other problems leading to the cascade.

Assessment of Transmission System Performance, Protection, Control, Maintenance, and Damage

This team investigated the causes of all transmission facility automatic operations (trips and reclosings) leading up to and through to the end of the cascade on all facilities greater than 100 kV. Included in the review were relay protection and remedial action schemes and identification of the cause of each operation and any misoperations that may have occurred. The team also assessed transmission facility maintenance practices in the affected area as compared to good utility practice and identified any transmission equipment that was damaged in any way as a result of the cascading outage. The team reported patterns and conclusions regarding what caused transmission facilities to trip; why did the cascade extend as far as it did and not further into other systems; any misoperations and the effect those misoperations had on the outage; and any transmission equipment damage. Also the team reported on the transmission facility maintenance practices of entities in the affected area compared to good utility practice.

Assessment of Generator Performance, Protection, Controls, Maintenance, and Damage

This team investigated the cause of generator trips for all generators with a 10 MW or greater nameplate rating leading to and through the end of the cascade. The review included the cause for the generator trips, relay targets, unit power runbacks, and voltage/reactive power excursions. The team reported any generator equipment that was damaged as a result of the cascading outage. The team reported on patterns and conclusions regarding what caused generation facilities to trip. The team

identified any unexpected performance anomalies or unexplained events. The team assessed generator maintenance practices in the affected area as compared to good utility practice. The team analyzed the coordination of generator under-frequency settings with transmission settings, such as under-frequency load shedding. The team gathered and analyzed data on affected nuclear units and worked with the Nuclear Regulatory Commission to address U.S. nuclear unit issues.

Assessment of Right of Way (ROW) Maintenance

The Vegetation/ROW Team investigated the practices of transmission facilities owners in the affected areas for vegetation management and ROW maintenance. These practices were compared to accepted utility practices in general across the Eastern Interconnection. Also, the team investigated historical patterns in the area related to outages caused by contact with vegetation.

Root Cause Analysis

The investigation team used an analytic technique called root cause analysis to help guide the overall investigation process by providing a systematic approach to evaluating root causes and contributing factors leading to the start of the cascade on August 14. The root cause analysis team worked closely with the technical investigation teams providing feedback and queries on additional information. Also, drawing on other data sources as needed, the root cause analysis verified facts regarding conditions and actions (or inactions) that contributed to the blackout.

Oversight and Coordination

The Task Force's U.S. and Canadian coordinators held frequent conference calls to ensure that all components of the investigation were making timely progress. They briefed both Secretary Abraham and Minister Dhaliwal regularly and provided weekly summaries from all components on the progress of the investigation. The leadership of the electric system investigation team held daily conference calls to address analytical and process issues through the investigation. The three Working Groups held weekly conference calls to enable the investigation team to update the Working Group members on the state of the overall analysis.

Root Cause Analysis

Root cause analysis is a systematic approach to identifying and validating causal linkages among conditions, events, and actions (or inactions) leading up to a major event of interest—in this case the August 14 blackout. It has been successfully applied in investigations of events such as nuclear power plant incidents, airplane crashes, and the recent Columbia space shuttle disaster.

Root cause analysis is driven by facts and logic. Events and conditions that may have helped to cause the major event in question must be described in factual terms. Causal linkages must be established between the major event and earlier conditions or events. Such earlier conditions or events must be examined in turn to determine their causes, and at each stage the investigators must ask whether a particular condition or event could have developed or occurred if a proposed cause (or combination of causes) had not been present. If the particular event being considered could have occurred without the proposed cause (or combination of causes), the proposed cause or combination of causes is dropped from consideration and other possibilities are considered.

Root cause analysis typically identifies several or even many causes of complex events; each of the various branches of the analysis is pursued until either a "root cause" is found or a non-correctable condition is identified. (A condition might be considered as non-correctable due to existing law, fundamental policy, laws of physics, etc.). Sometimes a key event in a causal chain leading to the major event could have been prevented by timely action by one or another party; if such action was feasible, and if the party had a responsibility to take such action, the failure to do so becomes a root cause of the major event.

Appendix B

List of Electricity Acronyms

BPA	Bonneville Power Administration
CNSC	Canadian Nuclear Safety Commission
DOE	Department of Energy (U.S.)
ECAR	East Central Area Reliability Coordination Agreement
ERCOT	Electric Reliability Council of Texas
FERC	Federal Energy Regulatory Commission (U.S.)
FRCC	Florida Reliability Coordinating Council
GW, GWh	Gigawatt, Gigawatt-hour
kV, kVAr	Kilovolt, Kilovolt-amperes-reactive
kW, kWh	Kilowatt, Kilowatt-hour
MAAC	Mid-Atlantic Area Council
MAIN	Mid-America Interconnected Network
MAPP	Mid-Continent Area Power Pool
MVA, MVAr	Megavolt-amperes, Megavolt-amperes-reactive
MW, MWh	Megawatt, Megawatt-hour
NERC	North American Electric Reliability Council
NPCC	Northeast Power Coordination Council
NRC	Nuclear Regulatory Commission (U.S.)
NRCan	Natural Resources Canada
OTD	Office of Transmission and Distribution (U.S. DOE)
PUC	Public Utility Commission (state)
RTO	Regional Transmission Organization
SERC	Southeast Electric Reliability Council
SPP	Southwest Power Pool
TVA	Tennessee Valley Authority (U.S.)

Appendix C

Electricity Glossary

AC: Alternating current; current that changes periodically (sinusoidally) with time.

ACE: Area Control Error in MW. A negative value indicates a condition of under-generation relative to system load and imports, and a positive value denotes over-generation.

Active Power: Also known as "real power." The rate at which work is performed or that energy is transferred. Electric power is commonly measured in watts or kilowatts. The terms "active" or "real" power are often used in place of the term power alone to differentiate it from reactive power. The rate of producing, transferring, or using electrical energy, usually expressed in kilowatts (kW) or megawatts (MW).

Adequacy: The ability of the electric system to supply the aggregate electrical demand and energy requirements of customers at all times, taking into account scheduled and reasonably expected unscheduled outages of system elements.

AGC: Automatic Generation Control is a computation based on measured frequency and computed economic dispatch. Generation equipment under AGC automatically respond to signals from an EMS computer in real time to adjust power output in response to a change in system frequency, tie-line loading, or to a prescribed relation between these quantities. Generator output is adjusted so as to maintain a target system frequency (usually 60 Hz) and any scheduled MW interchange with other areas.

Apparent Power: The product of voltage and current phasors. It comprises both active and reactive power, usually expressed in kilovoltamperes (kVA) or megavoltamperes (MVA).

Automatic Operating Systems: Special protection systems, or remedial action schemes, that require no intervention on the part of system operators.

Blackstart Capability: The ability of a generating unit or station to go from a shutdown condition to an operating condition and start delivering power without assistance from the electric system.

Bulk Electric System: A term commonly applied to the portion of an electric utility system that encompasses the electrical generation resources and bulk transmission system.

Bulk Transmission: A functional or voltage classification relating to the higher voltage portion of the transmission system, specifically, lines at or above a voltage level of 115 kV.

Bus: Shortened from the word busbar, meaning a node in an electrical network where one or more elements are connected together.

Capacitor Bank: A capacitor is an electrical device that provides reactive power to the system and is often used to compensate for reactive load and help support system voltage. A bank is a collection of one or more capacitors at a single location.

Capacity: The rated continuous load-carrying ability, expressed in megawatts (MW) or megavolt-amperes (MVA) of generation, transmission, or other electrical equipment.

Cascading: The uncontrolled successive loss of system elements triggered by an incident at any location. Cascading results in widespread service interruption, which cannot be restrained from sequentially spreading beyond an area predetermined by appropriate studies.

Circuit: A conductor or a system of conductors through which electric current flows.

Circuit Breaker: A switching device connected to the end of a transmission line capable of opening or closing the circuit in response to a command, usually from a relay.

Control Area: An electric power system or combination of electric power systems to which a common automatic control scheme is applied in order to: (1) match, at all times, the power output of the generators within the electric power system(s) and capacity and energy purchased from entities outside the electric power system(s), with the load in the electric power system(s); (2) maintain, within the limits of Good Utility Practice, scheduled interchange with other Control Areas; (3) maintain the frequency of the electric power system(s) within reasonable limits in accordance with Good Utility Practice; and (4) provide sufficient

generating capacity to maintain operating reserves in accordance with Good Utility Practice.

Contingency: The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch, or other electrical element. A contingency also may include multiple components, which are related by situations leading to simultaneous component outages.

Control Area Operator: An individual or organization responsible for controlling generation to maintain interchange schedule with other control areas and contributing to the frequency regulation of the interconnection. The control area is an electric system that is bounded by interconnection metering and telemetry.

Current (Electric): The rate of flow of electrons in an electrical conductor measured in Amperes.

DC: Direct current; current that is steady and does not change with time.

Dispatch Operator: Control of an integrated electric system involving operations such as assignment of levels of output to specific generating stations and other sources of supply; control of transmission lines, substations, and equipment; operation of principal interties and switching; and scheduling of energy transactions.

Distribution Network: The portion of an electric system that is dedicated to delivering electric energy to an end user, at or below 69 kV. The distribution network consists primarily of low-voltage lines and transformers that "transport" electricity from the bulk power system to retail customers.

Disturbance: An unplanned event that produces an abnormal system condition.

Electrical Energy: The generation or use of electric power by a device over a period of time, expressed in kilowatthours (kWh), megawatthours (MWh), or gigawatthours (GWh).

Electric Utility Corporation: Person, agency, authority, or other legal entity or instrumentality that owns or operates facilities for the generation, transmission, distribution, or sale of electric energy primarily for use by the public, and is defined as a utility under the statutes and rules by which it is regulated. An electric utility can be investor-owned, cooperatively owned, or government-owned (by a federal agency, crown corporation, State, provincial government, municipal government, and public power district).

Emergency: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit loss of transmission facilities or generation supply that could adversely affect the reliability of the electric system.

Emergency Voltage Limits: The operating voltage range on the interconnected systems that is acceptable for the time, sufficient for system adjustments to be made following a facility outage or system disturbance.

EMS: An Energy Management System is a computer control system used by electric utility dispatchers to monitor the real time performance of various elements of an electric system and to control generation and transmission facilities.

Fault: A fault usually means a short circuit, but more generally it refers to some abnormal system condition. Faults occur as random events, usually an act of nature.

Federal Energy Regulatory Commission (FERC): Independent Federal agency within the U.S. Department of Energy that, among other responsibilities, regulates the transmission and wholesale sales of electricity in interstate commerce.

Flashover: A plasma arc initiated by some event such as lightning. Its effect is a short circuit on the network.

Flowgate: A single or group of transmission elements intended to model MW flow impact relating to transmission limitations and transmission service usage.

Forced Outage: The removal from service availability of a generating unit, transmission line, or other facility for emergency reasons or a condition in which the equipment is unavailable due to unanticipated failure.

Frequency: The number of complete alternations or cycles per second of an alternating current, measured in Hertz. The standard frequency in the United States is 60 Hz. In some other countries the standard is 50 Hz.

Frequency Deviation or Error: A departure from scheduled frequency. The difference between actual system frequency and the scheduled system frequency.

Frequency Regulation: The ability of a Control Area to assist the interconnected system in maintaining scheduled frequency. This assistance can include both turbine governor response and automatic generation control.

Frequency Swings: Constant changes in frequency from its nominal or steady-state value.

Generation (Electricity): The process of producing electrical energy from other forms of energy; also, the amount of electric energy produced, usually expressed in kilowatt hours (kWh) or megawatt hours (MWh).

Generator: Generall, an electromechanical device used to convert mechanical power to electrical power.

Grid: An electrical transmission and/or distribution network.

Grid Protection Scheme: Protection equipment for an electric power system, consisting of circuit breakers, certain equipment for measuring electrical quantities (e.g., current and voltage sensors) and devices called relays. Each relay is designed to protect the piece of equipment it has been assigned from damage. The basic philosophy in protection system design is that any equipment that is threatened with damage by a sustained fault is to be automatically taken out of service.

Ground: A conducting connection between an electrical circuit or device and the earth. A ground may be intentional, as in the case of a safety ground, or accidental, which may result in high overcurrents.

Imbalance: A condition where the generation and interchange schedules do not match demand.

Impedance: The total effects of a circuit that oppose the flow of an alternating current consisting of inductance, capacitance, and resistance. It can be quantified in the units of ohms.

Independent System Operator (ISO): An organization responsible for the reliable operation of the power grid under its purview and for providing open transmission access to all market participants on a nondiscriminatory basis. An ISO is usually not-for-profit and can advise other utilities within its territory on transmission expansion and maintenance but does not have the responsibility to carry out the functions.

Interchange: Electric power or energy that flows across tie-lines from one entity to another, whether scheduled or inadvertent.

Interconnected System: A system consisting of two or more individual electric systems that normally operate in synchronism and have connecting tie lines.

Interconnection: When capitalized, any one of the five major electric system networks in North America: Eastern, Western, ERCOT (Texas), Québec, and Alaska. When not capitalized, the facilities that connect two systems or Control Areas. Additionally, an interconnection refers to the facilities that connect a nonutility generator to a Control Area or system.

Interface: The specific set of transmission elements between two areas or between two areas comprising one or more electrical systems.

Island: A portion of a power system or several power systems that is electrically separated from the interconnection due to the disconnection of transmission system elements.

Kilovar (kVAr): Unit of alternating current reactive power equal to 1,000 VArs.

Kilovolt (kV): Unit of electrical potential equal to 1,000 Volts.

Kilovolt-Amperes (kVA): Unit of apparent power equal to 1,000 volt amperes. Here, apparent power is in contrast to real power. On ac systems the voltage and current will not be in phase if reactive power is being transmitted.

Kilowatthour (kWh): Unit of energy equaling one thousand watthours, or one kilowatt used over one hour. This is the normal quantity used for metering and billing electricity customers. The price for a kWh varies from approximately 4 cents to 15 cents. At a 100% conversion efficiency, one kWh is equivalent to about 4 fluid ounces of gasoline, 3/16 pound of liquid petroleum, 3 cubic feet of natural gas, or 1/4 pound of coal.

Line Trip: Refers to the automatic opening of the conducting path provided by a transmission line by the circuit breakers. These openings or "trips" are designed to protect the transmission line during faulted conditions.

Load (Electric): The amount of electric power delivered or required at any specific point or points on a system. The requirement originates at the energy-consuming equipment of the consumers. Load should not be confused with demand, which is the measure of power that a load receives or requires. See "Demand."

Load Shedding: The process of deliberately removing (either manually or automatically) preselected customer demand from a power system in response to an abnormal condition, to maintain the integrity of the system and minimize overall customer outages.

Lockout: A state of a transmission line following breaker operations where the condition detected by the protective relaying was not eliminated by temporarily opening and reclosing the line, possibly multiple times. In this state, the circuit breakers cannot generally be reclosed without resetting a lockout device.

Market Participant: An entity participating in the energy marketplace by buying/selling transmission rights, energy, or ancillary services into, out of, or through an ISO-controlled grid.

Megawatthour (MWh): One million watthours.

NERC Interregional Security Network (ISN): A communications network used to exchange electric system operating parameters in near real time among those responsible for reliable operations of the electric system. The ISN provides timely and accurate data and information exchange among reliability coordinators and other system operators. The ISN, which operates over the frame relay NERCnet system, is a private Intranet that is capable of handling additional applications between participants.

Normal (Precontingency) Operating Procedures: Operating procedures that are normally invoked by the system operator to alleviate potential facility overloads or other potential system problems in anticipation of a contingency.

Normal Voltage Limits: The operating voltage range on the interconnected systems that is acceptable on a sustained basis.

North American Electric Reliability Council **(NERC):** A not-for-profit company formed by the electric utility industry in 1968 to promote the reliability of the electricity supply in North America. NERC consists of nine Regional Reliability Councils and one Affiliate, whose members account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico. The members of these Councils are from all segments of the electricity supply industry: investor-owned, federal, rural electric cooperative, state/municipal, and provincial utilities, independent power producers, and power marketers. The NERC Regions are: East Central Area Reliability Coordination Agreement (ECAR); Electric Reliability Council of Texas (ERCOT); Mid-Atlantic Area Council (MAAC); Mid-America Interconnected Network (MAIN); Mid-Continent Area Power Pool (MAPP); Northeast Power Coordinating Council (NPCC); Southeastern Electric Reliability Council (SERC); Southwest Power Pool (SPP); Western Systems Coordinating Council (WSCC); and Alaskan Systems Coordination Council (ASCC, Affiliate).

Operating Criteria: The fundamental principles of reliable interconnected systems operation, adopted by NERC.

Operating Guides: Operating practices that a Control Area or systems functioning as part of a Control Area may wish to consider. The application of Guides is optional and may vary among Control Areas to accommodate local conditions and individual system requirements.

Operating Policies: The doctrine developed for interconnected systems operation. This doctrine consists of Criteria, Standards, Requirements, Guides, and instructions, which apply to all Control Areas.

Operating Procedures: A set of policies, practices, or system adjustments that may be automatically or manually implemented by the system operator within a specified time frame to maintain the operational integrity of the interconnected electric systems.

Operating Requirements: Obligations of a Control Area and systems functioning as part of a Control Area.

Operating Standards: The obligations of a Control Area and systems functioning as part of a Control Area that are measurable. An Operating Standard may specify monitoring and surveys for compliance.

Outage: The period during which a generating unit, transmission line, or other facility is out of service.

Post-contingency Operating Procedures: Operating procedures that may be invoked by the system operator to mitigate or alleviate system problems after a contingency has occurred.

Protective Relay: A device designed to detect abnormal system conditions, such as electrical shorts on the electric system or within generating plants, and initiate the operation of circuit breakers or other control equipment.

Power/Phase Angle: The angular relationship between an ac (sinusoidal) voltage across a circuit element and the ac (sinusoidal) current through it. The real power that can flow is related to this angle.

Power: See "Active Power."

Reactive Power: The portion of electricity that establishes and sustains the electric and magnetic fields of alternating-current equipment. Reactive power must be supplied to most types of magnetic equipment, such as motors and transformers. It also must supply the reactive losses on transmission facilities. Reactive power is provided by generators, synchronous condensers, or electrostatic equipment such as capacitors and directly influences electric system voltage. It is usually expressed in kilovars (kVAr) or megavars (MVAr). The mathematical product of voltage and current consumed by reactive loads. Examples of reactive loads include capacitors and inductors. These types of loads, when connected to an ac voltage source, will draw current, but because the current is 90 degrees out of phase with the applied voltage, they actually consume no real power in the ideal sense.

Real Power: See "Active Power."

Regional Transmission Operator (RTO): An organization that is independent from all generation and power marketing interests and has exclusive responsibility for electric transmission grid operations, short-term electric reliability, and transmission services within a multi-State region. To achieve those objectives, the RTO manages transmission facilities owned by different companies and encompassing one, large, contiguous geographic area.

Relay: A device that controls the opening and subsequent reclosing of circuit breakers. Relays take measurements from local current and voltage transformers, and from communication channels connected to the remote end of the lines. A relay output trip signal is sent to circuit breakers when needed.

Relay Setting: The parameters that determine when a protective relay will initiate operation of circuit breakers or other control equipment.

Reliability: The degree of performance of the elements of the bulk electric system that results in electricity being delivered to customers within accepted standards and in the amount desired. Reliability may be measured by the frequency, duration, and magnitude of adverse effects on the electric supply. Electric system reliability can be addressed by considering two basic and functional aspects of the electric system Adequacy and Security.

Reliability Coordinator: An individual or organization responsible for the safe and reliable operation of the interconnected transmission system for their defined area, in accordance with NERC reliability standards, regional criteria, and subregional criteria and practices.

Resistance: The characteristic of materials to restrict the flow of current in an electric circuit. Resistance is inherent in any electric wire, including those used for the transmission of electric power. Resistance in the wire is responsible for heating the wire as current flows through it and the subsequent power loss due to that heating.

Restoration: The process of returning generators and transmission system elements and restoring load following an outage on the electric system.

Safe Limits: System limits on quantities such as voltage or power flows such that if the system is operated within these limits it is secure and reliable.

SCADA: Supervisory Control and Data Acquisition system; a system of remote control and telemetry used to monitor and control the electric system.

Scheduling Coordinator: An entity certified by the ISO for the purpose of undertaking scheduling functions.

Security: The ability of the electric system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system elements.

Security Coordinator: An individual or organization that provides the security assessment and emergency operations coordination for a group of Control Areas.

Short Circuit: A low resistance connection unintentionally made between points of an electrical circuit, which may result in current flow far above normal levels.

Single Contingency: The sudden, unexpected failure or outage of a system facility(s) or element(s) (generating unit, transmission line, transformer, etc.). Elements removed from service as part of the operation of a remedial action scheme are considered part of a single contingency.

Special Protection System: An automatic protection system designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components.

Stability: The ability of an electric system to maintain a state of equilibrium during normal and abnormal system conditions or disturbances.

Stability Limit: The maximum power flow possible through a particular point in the system while maintaining stability in the entire system or the part of the system to which the stability limit refers.

State Estimator: Computer software that takes redundant measurements of quantities related to system state as input and provides an estimate of the system state (bus voltage phasors). It is used to confirm that the monitored electric power system is operating in a secure state by simulating the system both at the present time and one step ahead, for a particular network topology and loading condition. With the use of a state estimator and its associated contingency analysis software, system operators can review each critical contingency to determine whether each possible future state is within reliability limits.

Station: A node in an electrical network where one or more elements are connected. Examples include generating stations and substations.

Substation: Facility equipment that switches, changes, or regulates electric voltage.

Subtransmission: A functional or voltage classification relating to lines at voltage levels between 69kV and 115kV.

Supervisory Control and Data Acquisition (SCADA): See SCADA.

Surge: A transient variation of current, voltage, or power flow in an electric circuit or across an electric system.

Surge Impedance Loading: The maximum amount of real power that can flow down a lossless transmission line such that the line does not require any VArs to support the flow.

Switching Station: Facility equipment used to tie together two or more electric circuits through switches. The switches are selectively arranged to permit a circuit to be disconnected, or to change the electric connection between the circuits.

Synchronize: The process of connecting two previously separated alternating current apparatuses after matching frequency, voltage, phase angles, etc. (e.g., paralleling a generator to the electric system).

System: An interconnected combination of generation, transmission, and distribution components comprising an electric utility and independent power producer(s) (IPP), or group of utilities and IPP(s).

System Operator: An individual at an electric system control center whose responsibility it is to monitor and control that electric system in real time.

System Reliability: A measure of an electric system's ability to deliver uninterrupted service at the proper voltage and frequency.

Thermal Limit: A power flow limit based on the possibility of damage by heat. Heating is caused by the electrical losses which are proportional to the square of the *active power* flow. More precisely, a thermal limit restricts the sum of the squares of *active* and *reactive power*.

Tie-line: The physical connection (e.g. transmission lines, transformers, switch gear, etc.) between two electric systems that permits the transfer of electric energy in one or both directions.

Time Error: An accumulated time difference between Control Area system time and the time standard. Time error is caused by a deviation in Interconnection frequency from 60.0 Hertz.

Time Error Correction: An offset to the Interconnection's scheduled frequency to correct for the time error accumulated on electric clocks.

Transfer Limit: The maximum amount of power that can be transferred in a reliable manner from one area to another over all transmission lines (or paths) between those areas under specified system conditions.

Transformer: A device that operates on magnetic principles to increase (step up) or decrease (step down) voltage.

Transient Stability: The ability of an electric system to maintain synchronism between its parts when subjected to a disturbance of specified severity and to regain a state of equilibrium following that disturbance.

Transmission: An interconnected group of lines and associated equipment for the movement or transfer of electric energy between points of supply and points at which it is transformed for delivery to customers or is delivered to other electric systems.

Transmission Loading Relief (TLR): A procedure used to manage congestion on the electric transmission system.

Transmission Margin: The difference between the maximum power flow a transmission line can handle and the amount that is currently flowing on the line.

Transmission Operator: NERC-certified person responsible for monitoring and assessing local reliability conditions, who operates the transmission facilities, and who executes switching orders in support of the Reliability Authority.

Transmission Overload: A state where a transmission line has exceeded either a normal or emergency rating of the electric conductor.

Transmission Owner (TO) or Transmission Provider: Any utility that owns, operates, or controls facilities used for the transmission of electric energy.

Trip: The opening of a circuit breaker or breakers on an electric system, normally to electrically isolate a particular element of the system to prevent it from being damaged by fault current or other potentially damaging conditions. See Line Trip for example.

Voltage: The electrical force, or "pressure," that causes current to flow in a circuit, measured in Volts.

Voltage Collapse (decay): An event that occurs when an electric system does not have adequate reactive support to maintain voltage stability. Voltage Collapse may result in outage of system elements and may include interruption in service to customers.

Voltage Control: The control of transmission voltage through adjustments in generator reactive output and transformer taps, and by switching capacitors and inductors on the transmission and distribution systems.

Voltage Limits: A hard limit above or below which is an undesirable operating condition. Normal limits are between 95 and 105 percent of the nominal voltage at the bus under discussion.

Voltage Reduction: A procedure designed to deliberately lower the voltage at a bus. It is often used as a means to reduce demand by lowering the customer's voltage.

Voltage Stability: The condition of an electric system in which the sustained voltage level is controllable and within predetermined limits.

Watthour (Wh): A unit of measure of electrical energy equal to 1watt of power supplied to, or taken from, an electric circuit steadily for 1 hour.

Appendix D

Transmittal Letters from the Three Working Groups

Mr. James W. Glotfelty
Director, Office of Electric Transmission
and Distribution
U.S. Department of Energy
1000 Independence Avenue SW
Washington, DC 20585

Dr. Nawal Kamel
Special Assistant to the Deputy Minister
Natural Resources Canada
580 Booth Street
Ottawa, ON
K1A 0E4

Dear Mr. Glotfelty and Dr. Kamel:

Enclosed is the Interim Report of the Electric System Working Group (ESWG) supporting the United States - Canada Power System Outage Task Force.

This report presents the results of an intensive and thorough investigation by a bi-national team of the causes of the blackout that occurred on August 14, 2003. The report was written largely by four members of the Working Group (Joe Eto, David Meyer, Alison Silverstein, and Tom Rusnov), with important assistance from many members of the Task Force's investigative team. Other members of the ESWG reviewed the report in draft and provided valuable suggestions for its improvement. Those members join us in this submittal and have signed on the attached page. Due to schedule conflicts, one member of the ESWG was not able to participate in the final review of the report and has not signed this transmittal letter for that reason.

Sincerely,

David H. Meyer

David H. Meyer
Senior Advisor
U.S. Department
of Energy
Co-Chair, ESWG

Thomas Rusnov
Senior Advisor
Natural Resources
Canada
Co-Chair, ESWG

alison silverstein

Alison Silverstein
Senior Energy Policy Advisor
to the Chairman
Federal Energy Regulatory
Commission
Co-Chair, ESWG

David Burpee, Director,
Renewable and Electrical Energy Division
Natural Resources Canada

Donald Downes, Chairman
Connecticut Department of
Public Utility Control

Joseph Eto, Staff Scientist
U.S. Department of Energy
Lawrence Berkeley National Laboratory
Consortium for Electric Reliability
Technology Solutions

Jeanne Fox, President
New Jersey Board of Public Utilities

H. Kenneth Haase
Senior Vice President, Transmission
New York Power Authority

Gene Whitney, Policy Analyst
National Science and Technology Council
U.S. Office of Science and Technology
Policy
Executive Office of the President

Blaine Loper, Senior Engineer
Pennsylvania Public Utility Commission

(not able to participate in review)

William D. McCarty, Chairman
Indiana Utility Regulatory Commission

David McFadden
Chair, National Energy and Infrastructure
Industry Group
Gowlings, Lafleur, Henderson LLP
Ontario

David O'Brien, Commissioner
Vermont Department of Public Service

David O'Connor, Commissioner
Div. of Energy Resources
Massachusetts Office of Consumer Affairs
And Business Regulation

Alan Schriber, Chairman
Ohio Public Utilities Commission

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

CHAIRMAN

Canadian Nuclear Safety Commission
President and Chief Executive Officer

Commission canadienne de sûreté nucléaire
Présidente et première dirigeante

November 5, 2003

PREDECISIONAL

Mr. James Glotfelty
Senior Policy Advisor
Office of the Secretary
U.S. Department of Energy
1000 Independence Ave., Suite 7B-222
Washington, DC 20585

Dr. Nawal Kamel
Special Assistant to the Deputy Minister
Natural Resources Canada
580 Booth Street
Ottawa, ON
K1A 0E4

Dear Mr. Glotfelty and Dr. Kamel:

Enclosed for incorporation into the Task Force report is the interim phase-one report of the Nuclear Working Group supporting the United States - Canada Joint Power System Outage Task Force. The members of the Nuclear Working Group join us in this submittal and have signed the attached pages. This interim report is predecisional (not for public release) until you issue the Task Force interim report, and should be made available only to those individuals needing this information to support the Task Force activities.

Please provide any comments related to the Canadian nuclear plants to either Mr. Jim Blyth (613-995-2655; blythj@cnsc-ccsn.gc.ca), or Mark Dallaire (613-947-0957; dallairem@cnsc-ccsn.gc.ca). Comments on the U.S. nuclear plants should be directed to either Mr. Cornelius Holden (301-415-3036; cfh@nrc.gov) or Mr John Boska (301-415-2901; jpb1@nrc.gov).

Sincerely,

Nils J. Diaz
Chairman
U.S. Nuclear Regulatory Commission
U.S. Co-chair, Nuclear Working Group

Linda J. Keen
President and Chief Executive Officer
Canadian Nuclear Safety Commission
Canadian Co-chair, Nuclear Working Group

Enclosures: Nuclear Working Group Signature Pages (2)
Nuclear Working Group Interim Report Phase One

PREDECISIONAL

PREDECISIONAL

cc w/encl: Mr. James Blyth
Director General, Reactor Power Regulation
Canadian Nuclear Safety Commission

Mr. Samuel J. Collins
Deputy Executive Director, Reactor Programs
U.S. Nuclear Regulatory Commission

PREDECISIONAL

The members of the Nuclear Working Group hereby submit this report as input to the United States - Canada Joint Power System Outage Task Force:

Nils J. Diaz, Chairman
U.S. Nuclear Regulatory Commission
Co-chair, Nuclear Working Group

Samuel J. Collins, Deputy Executive Director
for Reactor Programs
U.S. Nuclear Regulatory Commission

William D. Magwood, IV, Director, Office of
Nuclear Energy, Science and Technology
U.S. Department of Energy

Edward Wilds, Bureau of Air Management,
Department of Environmental Protection
(Connecticut)

David O'Connor, Commissioner, Division of
Energy Resources, Office of Consumer
Affairs and Business Regulation
(Massachusetts)

J. Peter Lark, Chairman, Public Service
Commission (Michigan)

Frederick F. Butler, Commissioner, New
Jersey Board of Public Utilities (New Jersey)

Paul Eddy, Power Systems Operations
Specialist, Public Service Commission (New
York)

Dr. G. Ivan Maldonado, Associate Professor,
Mechanical, Industrial and Nuclear
Engineering; University of Cincinnati (Ohio)

David J. Allard, CHP, Director, Bureau of
Radiation Protection, Department of
Environmental Protection (Pennsylvania)

David O'Brien, Commissioner
Department of Public Service (Vermont)

The members of the Nuclear Working Group hereby submit this report as input to the United States - Canada Joint Power System Outage Task Force:

Linda J. Keen
President and Chief Executive Officer
Canadian Nuclear Safety Commission
Co-chair, Nuclear Working Group

James Blyth
Director-General, Directorate of Power Reactor Regulation
Canadian Nuclear Safety Commission

Ken Pereira
Vice-President, Operations Branch
Canadian Nuclear Safety Commission

Dr. Robert Morrison
Senior Advisor to the Deputy Minister
Natural Resources Canada

Duncan Hawthorne
Chief Executive Officer
Bruce Power
(Representing the Province of Ontario)

Mr. James W. Glotfelty
Director, Office of Electric Transmission
and Distribution
U.S. Department of Energy
1000 Independence Avenue SW
Washington, DC 20585

Dr. Nawal Kamel
Special Assistant to the Deputy Minister
Natural Resources Canada
580 Booth Street
Ottawa, ON
K1A 0E4

Dear Mr. Glotfelty and Dr. Kamel:

Enclosed is the Interim Report of the Security Working Group (SWG) supporting the United States - Canada Power System Outage Task Force.

The SWG Interim Report presents the results of the Working Group`s analysis to date of the security aspects of the power outage that occurred on August 14, 2003. This report comprises input from public sector, private sector, and academic members of the SWG, with important assistance from many members of the Task Force's investigative team. As co-chairs of the Security Working Group, we represent all members of the SWG in this submittal and have signed below.

Sincerely,

Bob Liscouski
Assistant Secretary for
Infrastructure Protection,
U.S. Department of Homeland Security
Co-Chair, SWG

William J.S. Elliott
Assistant Secretary to the Cabinet,
Security and Intelligence,
Privy Council Office
Government of Canada
Co-Chair, SWG

Attachment 1:

U.S.-Canada Power System Outage Task Force SWG Steering Committee members:

Bob Liscouski, Assistant Secretary for Infrastructure Protection, Department of Homeland Security (U.S. Government) (Co-Chair)

William J.S. Elliott, Assistant Secretary to the Cabinet, Security and Intelligence, Privy Council Office (Government of Canada) (Co-Chair)

U.S. Members

Andy Purdy, Deputy Director, National Cyber Security Division, Department of Homeland Security

Hal Hendershot, Acting Section Chief, Computer Intrusion Section, FBI

Steve Schmidt, Section Chief, Special Technologies and Applications, FBI

Kevin Kolevar, Senior Policy Advisor to the Secretary, DoE

Simon Szykman, Senior Policy Analyst, U.S. Office of Science &Technology Policy, White House

Vincent DeRosa, Deputy Commissioner, Director of Homeland Security (Connecticut)

Richard Swensen, Under-Secretary, Office of Public Safety and Homeland Security (Massachusetts)

Colonel Michael C. McDaniel (Michigan)

Sid Caspersen, Director, Office of Counter-Terrorism (New Jersey)

James McMahon, Senior Advisor (New York)

John Overly, Executive Director, Division of Homeland Security (Ohio)

Arthur Stephens, Deputy Secretary for Information Technology, (Pennsylvania)

Kerry L. Sleeper, Commissioner, Public Safety (Vermont)

Canada Members

James Harlick, Assistant Deputy Minister, Office of Critical Infrastructure Protection and Emergency Preparedness

Michael Devaney, Deputy Chief, Information Technology Security Communications Security Establishment

Peter MacAulay, Officer, Technological Crime Branch of the Royal Canadian Mounted Police

Gary Anderson, Chief, Counter-Intelligence – Global, Canadian Security Intelligence Service

Dr. James Young, Commissioner of Public Security, Ontario Ministry of Public Safety and Security